Tesis doctoral / Doctoral thesis

EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN EL ÁMBITO SANITARIO CONECTADO: ESPECIAL REFERENCIA A LAS PERSONAS MAYORES CON DISCAPACIDAD

THE RIGHT TO THE PROTECTION OF PERSONAL DATA IN THE CONNECTED HEALTH FIELD: SPECIAL REFERENCE TO ELDERLY PEOPLE WITH DISABILITIES

Doctoranda/PhD: IDOIA LANDA REZA

Directora/Director: ITZIAR ALKORTA IDIAKEZ

eman ta zabal zazu

Universidad del País Vasco

Euskal Herriko Unibertsitatea

Enero de 2023, January 2023

ETXEKOEI, MIKELI ETA LAGUNEI.

ESKERRIK ASKO BIHOTZ-BIHOTZEZ.

ÍNDICE

ABREVIATURAS

- **AEM** Agencia Europea de Medicamentos
- **AEPD** Agencia Española de Protección de Datos
- **APDCAT** Autoridad de Protección de Datos Catalana
- **APCPD** Asociación Profesional de Consultores en Protección de Datos
- **App** Aplicación móvil
- **AVPD** Agencia Vasca de Protección de Datos
- **BOE** Boletín Oficial Español
- **BOPV** Boletín Oficial del País Vasco
- **CBE** Comité de Bioética de España
- **CC** Código Civil
- **CdE** Consejo de Europa
- **CE** Constitución Española de 1978
- **CEDH** Convenio Europeo de Derechos Humanos
- **CERMI** Comité Español de Representantes de Personas con Discapacidad
- **CEPD** Comité Europeo de Protección de Datos
- **CIOMS** *Council for International Organizations of Medical Sciences* (Consejo de Organizaciones Internacionales de las Ciencias Médicas)
- **cit.** *Citato* (en la obra citada)
- **CNIL** *Commission nationale de l'informatique et des libertés* (Comisión Nacional de la Informática y las Libertades de Francia)
- **CDPD** Convención Internacional sobre los Derechos de las Personas con Discapacidad
- **CRPD** Comité sobre los Derechos de las Personas con Discapacidad
- **DA** Disposición Adicional
- **DPA** *Data Protection Act* (Ley de Protección de Datos de Irlanda)
- **DPD** Delegado de Protección de Datos

- **DPO** Data Protection Officer
- **DPC** *Data Protection Commission* (Comisión de Protección de Datos de Irlanda)
- **DOG** Diario Oficial de Galicia
- **DOUE** Diario Oficial de la Unión Europea
- **EDPS** *European Data Protection Supervisor* (Supervisor Europeo de Protección de Datos)
- **EEDS** Espacio Europeo de Datos Sanitarios
- **FDA** *Food and Drug Administration (*Administración de Alimentos y Medicamentos)
- **FRA** Agencia de los Derechos Fundamentales de la Unión Europea
- **GT29** Grupo del Trabajo del artículo 29
- **HC** Historial clínico
- **HCE** Historial clínico electrónico
- **HCDSNS** Historia Clínica Digital del Sistema Nacional de Salud
- **HRB** *Health Research Board* (Consejo de Investigación en Salud de Irlanda)
- **HRCDC** *Health Research Consent Declaration Committee (Comité de Declaración de Consentimiento de Investigación en Salud)*
- **HRR** *Health Research Regulation* (Reglamento de Investigación en Salud de Irlanda)
- **HSE** *Health Service Executive* (Ejecutivo de Servicios de Salud irlandés)
- **IA** Inteligencia artificial
- **Ibid.** Citado en la cita previa
- **ICO** *Information Commissioner's Office* (Oficina del Comisionado de Información del Reino Unido)
- **IdC** Internet de las Cosas
- **IdCM** Internet de las Cosas Médicas
- **ICS** *Irish Computer Society* (Sociedad Irlandesa de Informática)

- **INCIBE** Instituto Nacional de Ciberseguridad
- **INE** Instituto Nacional de Estadistica
- **IoMT** *Internet of Medical Things* (Internet de las cosas médicas)
- **IoT** *Internet of Things* (Internet de las cosas)
- **LBAP** Ley Básica de Autonomía del Paciente
- **LOPD** Ley Orgánica de Protección de Datos
- **LOPDGDD** Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales
- **LORTAD** Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal
- **NCHD** *Non Consultant Hospital Doctor* (médico de hospital no consultor)
- **NHS** *National Health Service* (Servicio Nacional de Salud del Reino Unido)
- **OMS** Organización Mundial de la Salud
- **ONU** Organización de Naciones Unidas
- **OPS** Organización Panamericana de Salud
- **PDA** *Personal Digital Assistant* (asistentes digitales personales)
- **pp.** Páginas
- **RAE** Real Academia de la lengua Española
- **RGPD** Reglamento General de Protección de Datos
- **SEPD** Supervisor Europeo de Protección de Datos
- **STC** Sentencia del Tribunal Constitucional
- **STEDH** Sentencia del Tribunal Europeo de Derechos Humanos
- **STJUE** Sentencia del Tribunal de Justicia de la Unión Europea
- **STS** Sentencia del Tribunal Supremo
- **TC** Tribunal Constitucional
- **TEDH** Tribunal Europeo de Derechos Humanos
- **TIC** Tecnologías de la Información y Comunicación

- TJUE	Tribunal de Justicia de la Unión Europea
- TS	Tribunal Supremo
- UE	Unión Europea
- UIT	Unión Internacional de Telecomunicaciones
- **UNESCO**	*United Nations Educational, Scientific and Cultural Organization* (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura)
- **UODO**	*Urząd Ochrony Danych Osobowych* (Autoridad de Protección de Datos de Polonia)

RESUMEN

La aplicación de las nuevas tecnologías de la información en el ámbito sanitario se ha presentado como una solución para hacer frente al envejecimiento poblacional en las sociedades occidentales, debido a que estas herramientas pueden garantizar el cuidado y la monitorización constante de las personas mayores al tiempo que prometen mejorar la calidad de la vida de las mismas, fomentando un envejecimiento más activo y saludable, lo cual cobra especial importancia en el caso de las personas mayores con discapacidad. El resultado de la suma de la tecnología emergente a los nuevos tratamientos de datos se traduce en un nuevo ámbito sanitario conectado. Sin embargo, la incorporación de estas nuevas herramientas puede crear una grave intromisión en la esfera privada de las personas mayores usuarias, especialmente aquellas que presentan algún grado de discapacidad ligada al deterioro cognitivo. Por ello, la extensión y normalización del uso de los aparatos conectados en sanidad debe condicionarse a que exista un equilibrio entre el beneficio que puede brindar el tratamiento de los datos relativos a la salud, tanto para la asistencia sanitaria como la investigación en salud, por una parte, y el derecho a la protección de datos personales de los interesados, por otra.

Palabras clave: Derecho a la protección de datos personales, datos relativos a la salud, sanidad, nuevas tecnologías, personas mayores y discapacidad.

ABSTRACT

The application of new information technologies in the health field has been presented as a solution to deal with population aging in western societies, because these tools can guarantee the care and constant monitoring of the elderly while, at the same time, they promise to improve their quality of life, promoting a more active and healthy ageing, which is especially important in the case of older people with disabilities. The result of the addition of emerging technology to new data processing translates into a new connected health field. However, the incorporation of these new tools can create a serious interference in the private sphere of the elderly users, especially those who have some degree of disability linked to cognitive deterioration. For this reason, the extension and standardization of the use of connected devices in healthcare must be conditional on the existence of a balance between the benefits that the processing of health-related data can provide, both for healthcare and for health research, for on the one hand, and the right to the protection of personal data of the interested parties, on the other.

Keywords: Right to the protection of personal data, health data, healthcare, new technologies, elderly people and disability.

INTRODUCCIÓN

Debido al incremento de la esperanza de vida y a la reducción de la tasa de natalidad, nuestra sociedad se enfrenta a un envejecimiento poblacional, con un importante impacto social y económico por la mayor incidencia de problemas de salud en este sector poblacional, como las enfermedades crónicas y las enfermedades mentales. Frente a esta realidad, la tendencia actual es la de prevenir o ralentizar el desarrollo de las enfermedades que tienen un impacto significativo en la calidad de vida de las personas mayores, generando asimismo ahorros en el costo de los servicios de salud a través de soluciones de base tecnológica.

En este aspecto, el sector de la salud ha experimentado una transformación digital con la llegada de las nuevas tecnologías como el Big Data, la inteligencia artificial, el internet de las cosas, las aplicaciones informáticas o el Cloud Computing. Estas nuevas herramientas han dado lugar a un nuevo paradigma en materia de cuidados, a saber, el ámbito sanitario conectado. El tratamiento de los datos relativos a la salud con fines de investigación en salud tiene un valor incalculable, por tratarse del trampolín que da acceso al conocimiento científico que permite, entre otras cuestiones, implantar tratamientos personalizados o planificar estrategias de salud pública, para lo cual las nuevas tecnologías constituyen un elemento esencial.

Mediante el uso de esta tecnología emergente, las personas de edad avanzada podrán vivir el mayor tiempo posible en sus hogares, mientras puedan valerse por sí mismas, retrasando su entrada en un entorno residencial, esto es, la aplicación de las nuevas tecnologías de información y comunicación en el ámbito sanitario puede mejorar la calidad de la vida de las personas mayores, fomentando un envejecimiento activo y saludable. Sin embargo, la doctrina ha puesto de manifiesto el riesgo de que el uso indiscriminado de las mismas pueda suponer una grave intromisión en la esfera privada de estas personas que a menudo están condicionadas por la brecha digital. Por ello, su implementación en el ámbito sanitario debe tener un límite: el derecho a la protección de datos personales de los titulares de los datos. El reto actual consiste en encontrar un equilibrio justo entre el beneficio que proporciona el tratamiento de los datos relativos a la salud mediante las nuevas tecnologías, tanto para proveer una asistencia sanitaria de mayor calidad como para avanzar en la investigación en salud, y el derecho a la protección de datos personales de los interesados. Si bien el tratamiento de los datos relativos a la salud es necesario y su valor es innegable, esto no significa que todo procesamiento que involucre dichos datos deba ser aceptable.

Por otra parte, el consentimiento del interesado ha constituido históricamente el núcleo del sistema europeo de protección de datos personales, y actualmente sigue siendo la principal base legitimadora para el tratamiento de los datos relativos a la salud. Sin embargo, el desarrollo tecnológico que se ha producido en los últimos años ha banalizado la prestación de dicho consentimiento a través de formas más blandas que llevan a prestarlo casi por defecto, poniendo con ello en tela de juicio su valor como base legitimadora para el tratamiento de los datos personales. En un mundo cada vez

más digital es preciso cuestionarse si el consentimiento, creado para proporcionar a cada persona un control sobre sus datos, sigue siendo una herramienta adecuada para proteger el derecho a la protección de datos personales del sujeto, o por el contrario debemos considerarlo una herramienta obsoleta que es preciso sustituir o al menos complementar, y en este último caso qué instrumentos jurídicos cabría emplear como alternativa.

Abundando en la idea de que el consentimiento del interesado esté en crisis, no queda claro qué valor cobra el consentimiento que pueda otorgar una persona mayor con discapacidad para el tratamiento de sus datos personales. En este sentido, el 2 de junio de 2021 entró en vigor la Ley 8/2021, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica[1]. La citada ley pretende adecuar el ordenamiento a la Convención Internacional sobre los derechos de las personas con discapacidad hecha en Nueva York el 13 de diciembre de 2006, cuyo artículo 12 proclama que las personas con discapacidad tienen capacidad jurídica en igualdad de condiciones con las demás en todos los aspectos de la vida, y obliga a los Estados miembros a adoptar medidas para proporcionar a estas personas el apoyo que puedan necesitar en el ejercicio de su capacidad jurídica. Ante este cambio normativo, surge la necesidad de analizar la respuesta que proporciona la nueva ley para la presente manifestación de la voluntad.

Además del consentimiento del interesado en relación al uso de sus datos para el tratamiento sanitario, en este trabajo de investigación nos referiremos al uso de los datos relativos a la salud para la investigación científica. En el ámbito de la investigación sanitaria, aunque el Reglamento 679/2016, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[2], en adelante RGPD, prometía armonizar el uso de datos para la investigación sanitaria, finalmente rebajó dichas expectativas reconociendo a los Estados miembros competencia para el desarrollo de normas propias en este ámbito. El legislador español ha desarrollado dicha remisión a través de la Disposición Adicional Decimoséptima de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)[3]. En cambio, otros ordenamientos han hecho un uso sustancialmente diferente de la habilitación normativa, como por ejemplo Italia, que ha regulado el tratamiento de datos relativos a la salud con fines de investigación en el capítulo VII de su Decreto legislativo 196/2003 de 30 de junio de 2003[4]; o Irlanda, que ha optado por regular el presente tratamiento específicamente en su Ley 314/2018 de Protección de Datos (Sección 36(2)

[1] BOE núm. 132, de 3 de junio de 2021
[2] DOUE núm. 119, de 4 de mayo de 2016
[3] BOE núm. 294, de 6 de diciembre de 2018
[4] "*DECRETO LEGISLATIVO 10 agosto 2018, n. 101, recante Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonchè alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (in G.U. 4 settembre 2018 n.205)"*

Investigación en Salud), que entró en vigor el 8 de agosto de 2018[5]. Las divergencias normativas hacen que, actualmente, siga precisándose un análisis exhaustivo de la remisión del RGPD que ponga de relieve el hecho de que la falta de una legislación homogénea en el campo de la investigación sanitaria, altamente internacionalizada, afecta a la transmisión de datos intraeuropea.

La crisis sanitaria generada por el COVID-19 ha remarcado el valor de las nuevas tecnologías tanto para frenar la propagación como para acelerar el proceso de diagnóstico y tratamiento de la enfermedad, pero también ha servido para reforzar la idea de que ha de existir un equilibrio entre el derecho fundamental a la protección de datos personales y la investigación científica. Como respuesta a la situación de emergencia sanitaria, los diversos países europeos no han seguido la misma trayectoria con el fin de encontrar el conocimiento oculto en los datos relativos a la salud, introduciendo excepciones a su normativa y utilizando distintas bases legitimadoras. Aun encontrándose ante el mismo escenario, cada país ha adoptado sus propias medidas en relación a la protección de los datos empleados en la lucha contra la pandemia, dando lugar un escenario heterogéneo.

Hasta aquí nos hemos referido a las cuestiones suscitadas por la necesidad de hallar una base jurídica adecuada para el tratamiento de los datos relativos a la salud tanto cuando se destinan a la investigación como al cuidado de su salud. En este trabajo nos referiremos también a los derechos que les asisten a los interesados una vez hayan otorgado el consentimiento para el tratamiento. Como resultado del avance tecnológico que se ha producido en los últimos años, el legislador europeo se ha visto compelido a crear nuevos derechos para que los titulares de los datos puedan ejercer su derecho a la protección de datos personales en relación con los tratamientos realizados por terceros en la presente realidad digital. De esta forma, tras la entrada en vigor del RGPD, los derechos del interesado descritos en los artículos 15 y 21 del RGPD han sufrido una transformación con respecto a la Directiva anterior, pasando de denominarse derechos ARCO a derechos ARSLPO (acceso, rectificación, supresión, olvido, limitación del tratamiento, portabilidad y oposición). Pese a su modernización, la aplicación de los derechos del interesado sigue planteando problemas debido a la escueta y poco ilustrativa redacción del reglamento. Además, la normativa es general y no contempla cómo han de ser interpretados los derechos en ámbitos tan específicos como el sanitario. En consecuencia, la problemática aumenta cuando se ha de comprender el apartado de política de protección de datos de un documento sanitario o de la página oficial de un centro de salud, puesto que dichas secciones suelen estar limitadas a reproducir lo dispuesto en el RGPD.

En cuanto a la finalidad de este trabajo, además del objetivo general de adquirir competencia como investigadora en materia jurídica, se pretende responder a los problemas jurídicos a los que se ha aludido en los párrafos anteriores, realizando una

[5] "*S.I.No. 314/2018-Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018 ("Iris Oifigiúil" of 29th January, 2021)"*

especial referencia al caso de las personas mayores con discapacidad. El orden en el que se tratarán las cuestiones referidas es el siguiente. En primer lugar analizaremos la base legitimadora del consentimiento del interesado, principal herramienta que legitima el tratamiento de los datos relativos a la salud, para averiguar si el reforzamiento de los requisitos del consentimiento por parte del nuevo Reglamento ha sido suficiente para convertir al consentimiento del interesado en un instrumento de control adecuado para los datos relativos a la salud, o si, como entiende parte de la doctrina, el consentimiento del interesado es una herramienta obsoleta en el actual mundo conectado.

Tras examinar el cambio que ha producido la Ley 8/2021, el segundo objetivo ha sido analizar, entre otras cuestiones, el otorgamiento del consentimiento del interesado por parte de las personas mayores con discapacidad para el tratamiento de los datos relativos a la salud y la posibilidad de implementar las nuevas tecnologías para el cuidado de la salud de las personas mayores con discapacidad sin su consentimiento.

El tercer objetivo ha consistido en estudiar las bases legitimadoras que identifica el RGPD para el tratamiento de los datos relativos a la salud en la investigación sanitaria, y cómo ha resuelto esta remisión normativa el legislador español, comparando este desarrollo con el modelo normativo italiano e irlandés. La elección de dichos ordenamiento está justificada en las diferencias que se aprecian entre las mismas, lo cual refleja claramente la falta de armonización en el ámbito de la investigación sanitaria. A su vez, teniendo en cuenta el momento histórico vivido en el que se ha realizado esta tesis, se han analizado los tratamientos de datos relativos a la salud con fines de investigación en el contexto de la pandemia en el estado español, italiano e irlandés para observar las diferencias de cada país a la hora de elegir una base legal que les permitiera realizar el tratamiento de los datos relativos a la salud.

Todo ello nos ha permitido efectuar algunas propuestas de *lege ferenda* encaminadas a armonizar las bases legales de la investigación con datos a nivel europeo. Entre las propuestas analizadas cabe destacar el formulario europeo de consentimiento para la cesión altruista de datos que ha surgido en el contexto de la creación del Espacio Europeo de Datos Sanitarios (EEDS), con la entrada en vigor del Reglamento 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022 relativo a la gobernanza de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)[6]. Las restantes vías para compartir datos con fines de investigación e innovación contempladas por el nuevo Reglamento que permiten el tratamiento de los datos relativos a la salud son de menor interés para este trabajo, y serán analizadas detalladamente en futuras investigaciones.

Por último, el cuarto objetivo ha sido exponer el cambio que ha supuesto la transformación de los derechos ARCO a los derechos ARSLPO, con el fin de estudiar cómo han de ser interpretados en el ámbito específico de la sanidad, y qué efecto ha tenido la Ley 8/2021 en el ejercicio de los mismos en el caso de las personas mayores

[6] DOUE núm. 152, de 3 de junio de 2022

con discapacidad. De la misma forma, se ha analizado el caso particular del ejercicio de los derechos tras el fallecimiento del interesado, y cómo puede reflejarse anticipadamente la voluntad del mismo para el tratamiento post mortem de sus datos relativos a la salud.

Como consecuencia de la natural limitación temporal en el que se debe abordar este primer trabajo de investigación de carácter eminentemente formativo, se ha optado por limitar el ámbito de nuestra investigación a abordar los problemas que plantean las tecnologías actualmente en uso en el ámbito sanitario, dejando para futuras investigaciones cuestiones relevantes planteadas por la ciberseguridad, o el "*blockchain"*.

Se identifican las siguientes cuestiones de investigación que constituyen el objeto fundamental del presente trabajo y que, además de estructurar el corpus de la investigación, servirán también para organizar las principales conclusiones presentadas como resultado del mismo:

1. ¿Es el consentimiento del interesado una herramienta de control adecuada para el interesado en la era digital?

2. ¿Pueden las personas mayores con discapacidad otorgar su consentimiento para el tratamiento de sus datos relativos a la salud?

3. ¿Pueden implementarse las nuevas tecnologías para el cuidado de la salud de las personas mayores con discapacidad sin su consentimiento?

4. ¿Cómo han resuelto la remisión del artículo 9.4 del RGPD los legisladores españoles, italianos e irlandeses?, ¿qué efecto tiene la falta de armonización en este ámbito?, ¿cómo han realizado el tratamiento de los datos relativos a la salud con fines de investigación los citado países en el contexto de la pandemia?

5. ¿Qué derechos tiene el interesado?, ¿cómo han de ser interpretados estos derechos en el ámbito sanitario?, ¿pueden ser ejercidos por representación?, ¿pueden ser ejercidos tras el fallecimiento del interesado?

La realización de la presente tesis ha coincidido en el tiempo con la participación en el proyecto europeo SMART-BEAR[7], como Personal Investigador Contratado de la Universidad del País Vasco (UPV/EHU) bajo la dirección de la Dra. ALKORTA IDIAKEZ. El proyecto cuenta con miembros de distintas universidades, centros de investigación tecnológica, dos grandes empresas tecnológicas y cinco servicios de salud públicos y privados a nivel europeo, y participan 5.000 voluntarios mayores de 65 años. El objetivo del estudio es integrar en la vida y los hogares de los participantes distintos

[7] Disponible en: https://www.smart-bear.eu/

dispositivos que permitan la recopilación continua de los datos de las personas mayores participantes, para, posteriormente, analizarlos y así obtener la evidencia necesaria con el fin de ofrecer intervenciones personalizadas que promuevan su vida saludable e independiente. El hecho de participar en un proyecto de este calibre permite identificar de una forma práctica diversos problemas que surgen al llevar a cabo un estudio que tenga como objeto el tratamiento de los datos relativos a la salud de personas de edad avanzada a nivel europeo, teniendo en cuenta la divergencias normativas de los países participantes. De esta forma, aunque no se trate de una tesis aplicada, la participación también ha servido como herramienta a la hora de delimitar los puntos a tratar en este trabajo.

Para la elaboración de esta tesis doctoral con mención internacional que ha sido realizada en el periodo de tres años a jornada completa respetando en todo momento los principios éticos que le han sido de aplicación, se ha efectuado un análisis exhaustivo de las siguientes fuentes: legislación, jurisprudencia y doctrina. Posteriormente, en base al conocimiento adquirido, se han redactado los cinco capítulos que conforman la tesis, volviendo nuevamente a consultar las citadas fuentes a la hora de su redacción, todo ello bajo la dirección de la Dra. ALKORTA IDIAKEZ, quien me ha apoyado y me ha alentado en este camino.

Debido a que el derecho a la protección de datos personales es el núcleo y la base del trabajo, el estudio del contenido jurídico se ha concluido con las numerosas resoluciones, dictámenes, informes, guías y recomendaciones del Comité Europeo de Protección de Datos, antiguo Grupo de Trabajo del Artículo 29 (GT29), y diversas autoridades de control como la Agencia Española de Protección de Datos o la Agencia Vasca de Protección de Datos a las que hago referencia en el apartado de fuentes primarias citadas.

En el ámbito de la formación, la asistencia a congresos y seminarios ha sido una actividad útil tanto para conocer y escuchar a investigadores de prestigio y doctorandos con intereses similares, como para exponer ante un público ilustre diversas hipótesis. Esta última función ha servido para identificar aspectos a tratar y adquirir habilidades como investigadora. Igualmente, la realización de varios cursos de formación multidisciplinares ha sido una forma para adquirir un conocimiento más amplio del ámbito de estudio.

Con el fin de analizar y comprender adecuadamente las normativas extranjeras, se han realizado dos estancias doctorales en el transcurso del doctorado en la Universidad Alma Mater Studorium de Bolonia (Italia) y en la Universidad Dublin City University de Dublín (Irlanda). Debiendo agradecer a las citadas universidades y a los académicos Dña. RAFFAELLA BRIGHI y D. EDOARDO CELESTE por sus orientaciones y su opinión en relación a las numerosas cuestiones que se han contrastado con ellos.

CAPÍTULO 1: LA IMPLEMENTACIÓN DE LAS NUEVAS HERRAMIENTAS TECNOLÓGICAS BASADAS EN DATOS EN EL ÁMBITO SANITARIO

1. INTRODUCCIÓN:

El ámbito sanitario se encuentra actualmente inmerso en una profunda y continua transformación, los cambios están siendo provocados por unos avances sin precedentes en el conocimiento de la biología molecular, que data de finales del siglo pasado, que debe añadirse más recientemente un segundo factor decisivo, la revolución digital[8]. La medicina tradicional, basada en el contacto directo con el paciente, está siendo complementada y en algunos casos sustituida, por la utilización de herramientas digitales que permiten telemonitorizar al paciente en tiempo real. Gracias a estas herramientas, están desapareciendo los límites entre hospitales, centros médicos, profesionales y países. Se puede afirmar, por tanto, que en la segunda década del siglo XXI se ha producido un cambio de paradigma, de la medicina tradicional analógica, al modelo actual de salud digital.

El uso de dispositivos móviles conectados que recaban constantemente datos del usuario constituye uno de los elementos más visibles de este cambio de paradigma. Pero, la nueva salud conectada va más allá del tratamiento del paciente, ya que sirve también a otros múltiples propósitos como la realización de estadísticas, el diseño de estrategia a largo plazo en materia de prestación sanitaria, la mejora de servicios y, sobre todo, la elaboración de tratamiento con mayor detalle y sofisticación que contribuyen a la medicina personalizada. El antiguo sistema se centraba en curar las enfermedades, mientras que el nuevo paradigma apunta a la prevención, centrándose en la previsión de comportamientos y de posibles evoluciones de la enfermedad así como en la prevención de las mismas.

Hasta hace pocos años, se requería que el profesional sanitario y el paciente se encontraran en el mismo lugar, en la actualidad, esto ya no es un requisito obligatorio. La monitorización del estado de salud que realizan los nuevos dispositivos y el correspondiente tratamiento de los datos recolectados que permite su posterior análisis permite avanzar hacia un nuevo concepto de la atención médica personalizada, la cual ha de ser comprendida como la adaptación del tratamiento médico a las características individuales de cada paciente. Esta característica cobra especial importancia en el caso de las personas mayores, sobre todo en el caso de los mayores que viven en entornos rurales, puesto que con ello se evitan desplazamientos e ingresos hospitalarios innecesarios.

Por otra parte, debe hacerse mención a una segunda transformación importante en materia de atención médica la cual se ha producido a partir de la publicación del Código de Núremberg publicado el 20 de agosto de 1947. Hasta mediado el siglo XX, el

[8] SACRISTÁN, J.A., *Medicina centrada en el paciente*, Unión Editorial: Fundación Lilly, Madrid, 2018, p. 35

modelo de la relación entre el paciente y el profesional sanitario ha sido paternalista; esta característica se acentuaba, además en el caso de las personas de edad avanzada con discapacidad, cuya voluntad debía ser sustituida en aras al interés superior de estas personas cuya interpretación correspondía a los clínicos y a sus allegados, pero rara vez se preguntaba al propio paciente mayor. Frente a este modelo paternalista o de sustitución, el nuevo modelo de relación médico-paciente debe promover una forma de toma de decisiones compartida y deliberativa. Es precisamente en este proceso de cambio de paradigma en el que se ha de localizar el nacimiento de la nueva figura del "paciente activo" o del "paciente empoderado", a saber, ciudadanos y ciudadanas capaces de responsabilizarse de sí mismos respecto de su estado de salud conjuntamente con los profesionales de la salud y con la voluntad de participar en el proceso de mejora de su enfermedad y de su calidad de vida a través del autocuidado[9]. No hay duda de que las nuevas herramientas digitales y los aplicativos personalizados constituyen una oportunidad para facilitar la implicación del paciente en su propio tratamiento y prevención.

En suma, el uso de estas nuevas herramientas puede hacer que la medicina del futuro sea más personalizada, participativa, predictiva y preventiva. Su adecuada aplicación posibilitaría un envejecimiento más activo y saludable, tal y como predica el nuevo paradigma de salud digital del Ministerio de salud[10], empoderando a este sector poblacional. Sin embargo, no podemos perder de vista que la implementación de estas tecnologías multiplica el riesgo de brechas de seguridad que ponen en riesgo la privacidad del paciente así como su autodeterminación informativa. No hay duda que, el uso de la tecnología digital basada en datos de salud, especialmente sensibles, tiene que cumplir en todo momento la normativa de protección de datos personales. Por este motivo, debe subrayarse la idea de que la protección de los datos personales de los pacientes se identifica como uno de los mayores desafíos al que se enfrenta el sector de la salud. El reto consiste en encontrar un equilibrio entre las ventajas que ofrece el tratamiento de los datos personales que se realiza mediante las nuevas herramientas, y el derecho a la protección de datos de los pacientes.

En el presente capítulo se analizarán las principales herramientas que se utilizan actualmente en el ámbito sanitario (el historial clínico electrónico, el internet de las cosas, las aplicaciones informáticas, el Big Data, el Cloud Computing y la inteligencia artificial), identificando los retos que plantea su uso desde la perspectiva del derecho a la protección de datos personales. Una vez se hayan estudiado las citadas herramientas separadamente, se pasará a analizar el nuevo concepto de la salud digital, que es el resultado de la aplicación de los instrumentos tecnológicos en el ámbito de la sanidad. Dado que la salud digital engloba a la salud móvil y a la telemedicina, en este apartado se analizarán los citados dos términos y se expondrán los riesgos que conllevan los mismos desde la perspectiva del derecho a la protección de datos personales.

[9] MESTRE GONZÁLEZ, A., "La autonomía del paciente con enfermedades crónicas: De paciente pasivo a paciente activo", *Enfermería clínica*, Vol. 24, Núm. 1, 2014, p. 67

[10] MINISTERIO DE SALUD., "Estrategia de salud digital", *sanidad.gob.es,* 2 de diciembre de 2021, disponible en: https://www.sanidad.gob.es/ciudadanos/pdf/Estrategia_de_Salud_Digital_del_SNS.pdf

2. LAS HERRAMIENTAS TECNOLÓGICAS EN LA SANIDAD Y SUS RETOS:

2.1.Historial clínico electrónico:

2.1.1. Concepto:

La historia clínica se ha definido doctrinalmente como un documento o registro[11] que contiene el conjunto de la información y de los datos relativos al proceso o procesos asistenciales del paciente. Por tanto, al agregarse cronológicamente todos los aspectos acerca de cada consulta o episodio clínico, la historia clínica constituye un documento biográfico relativo a la asistencia sanitaria de un paciente[12]. Desde otro punto de vista, también ha sido definida como la narración escrita en soporte papel o informático, clara, precisa, detallada y ordenada de todos los datos y conocimientos y observaciones tanto personales como familiares que se refieren a un paciente y que sirven de base para el seguimiento de su enfermedad o de su estado de salud en general[13]. Desde la perspectiva de los datos personales, es importante observar que la historia clínica contiene los antecedentes familiares y hábitos de un ser humano, su constitución, fisiología y psicología, el ambiente en el que se desarrolla su existencia y, algunos casos sus características genéticas, así como, la etiología y evolución de las enfermedades que padecerá a lo largo de la vida.

Como documento de valor legal, el artículo 3.1 del Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica[14], se indica que la historia clínica es el conjunto de documentos y registros informáticos que deberá contener de forma clara y concisa los datos, valoraciones e informaciones generados en cada uno de los procesos asistenciales a que se somete un o una paciente y en los que se recoge el estado de salud, la atención recibida y la evolución clínica de la persona. Por su parte, en el preámbulo del Decreto 272/1986 de 25 de noviembre de 1986 por el que se regula el uso de la Historia Clínica de los centros Hospitalarios de la Comunidad Autónoma del País Vasco[15], se recoge que la historia clínica es el documento donde se contiene toda la información de utilidad

[11] La historia clínica constituye el documento esencial de la práctica clínica. Las primeras historias clínicas completas están contenidas en los libros las Epidemias I y III del Corpus Hipocraticum. En la Edad Media, se recuperó su elaboración con los Consilea y se mantuvo a lo largo del renacimiento denominándose Observatio. Su contenido se completó a lo largo del siglo XVIII con el método anatomoclínico y ene l siglo XIX con el desarrollo de técnicas fisiopatológicas. En el siglo XX hubo un rápido crecimiento de pruebas complementarias con aumento de la complejidad de la historia clínica que se conviertió en multidisciplinar y de obligado cumplimiento. Por último, en el siglo XXI, la informatización de la historia clínica produjo cambios radicales. Véase al respecto: FOMBELLA POSADA, M.J. y CEREIJO QUINTEIRO, M.J., "Historia de la historia clínica", *Galicia Clínica*, Vol. 73, Núm.1, 2012, p. 21

[12] CANTERO RIVAS, R.; MARTÍNEZ AGUADO, L.C. y MORENO VERNIS, M., *La historia clínica*, Comares, Granada, 2002, p. 78

[13] GÓMEZ PIQUERAS, C., "Contenido, usos y finalidad de la historia clínica", *ponencia en la AEPD*, 25 de febrero de 2008, disponible en: https://www.redipd.org/sites/default/files/2020-01/ponencia3_250208.pdf

[14] BOVP núm. 65 de 29 de marzo de 2012

[15] BOVP núm. 242 de 6 de diciembre de 1986

clínica relativa al estado de salud o enfermedad de la población asistida en el hospital, siendo este al mismo tiempo un medio de comunicación muy valioso para transmitir esta información entre los distintos agentes que intervienen en el plan de asistencia al enfermo.

Respecto a su contenido, debe contener datos suficientes (administrativos, clínicos y de curso evolutivo) para identificar al paciente tanto individualmente como en su ambiente o contexto social. Es decir, debe contener toda aquella información que se considere significativa desde el punto de vista médico para el conocimiento veraz y actualizado del estado de salud del paciente. Dichos datos han de ser plasmados según el orden cronológico en que ocurrieron de forma que justifiquen el diagnóstico y garanticen una asistencia sanitaria adecuada[16]. Es fácil comprender que debido al carácter y amplio abanico de datos que se vuelcan en la historia clínica, esta se convierte en la herramienta esencial de la asistencia sanitaria.

El soporte físico tradicional de almacenamiento de la información sanitaria ha sido el papel, pero es sabido que los nuevos avances electrónicos han traído consigo una nueva forma de almacenar y visualizar la información. Las TIC han transformado la realidad de la historia clínica tradicional abriendo paso a la historia clínica digital. Esta evolución ha permitido enriquecer la historia clínica puesto que cada vez se cuenta con más información clínica, y esto hacía que el sistema tradicional en soporte papel se revelara insuficiente a efectos de contener la ingente cantidad de datos que reúnen hoy las historias clínicas.

La acumulación de datos relativos a la salud de los pacientes en las historias clínicas y su correcta conservación se erigen en elementos necesarios para poder hacer un seguimiento pertinente del estado de salud de las personas. De hecho, la supresión de datos relevantes de la historia clínica, cuestión que se analizará más adelante, puede llegar a afectar gravemente a los tratamientos sanitarios, y, en consecuencia, a la vida de las personas. La gestión de la asistencia y de los servicios sanitarios en atención primaria, en atención especializada y en urgencias exige necesariamente una acumulación masiva de información personal de los ciudadanos para garantizar su salud[17]. Más allá del uso asistencial, la historia clínica digital, sirve de instrumento de ayuda para la investigación, al hacer viable el análisis y comparación de muchos casos individuales, se puede llegar a definir lo que es propio de cada enfermedad, lo cual tiene una importante repercusión para el conjunto de la sociedad.

[16]CANTERO RIVAS, R.; MARTÍNEZ AGUADO, L.C. y MORENO VERNIS, M., *La historia clínica*, cit., p. 6

[17] TRONCOSO REIGADA, A., "La confidencialidad de la historia clínica", *Cuadernos de derecho público*, Núm. 27, 2006, pp. 45-46

2.1.2. Riesgos que plantea el historial clínico electrónico desde la perspectiva del derecho a la protección de datos personales:

Pese a las ventajas ya señaladas, el historial clínico electrónico contiene un significativo potencial intrusivo en un ámbito de la personalidad tan íntimo como la salud, el cual, si bien facilita el trabajo de los facultativos sanitarios, puede acarrear riesgos para los pacientes.

En primer lugar, además del peligro que puede suponer un ataque informático en la red sanitaria, las personas que trabajan en el propio sistema sanitario pueden crear riesgos. En este sentido, existen problemas con el perfil de acceso, las rotaciones, las guardias o la delegación de funciones hacen que en muchas ocasiones sea complicado crear perfiles de acceso estáticos, son numerosos los casos en que una profesional debe realizar un acceso que en un inicio no le correspondía. El personal operativo tiene acceso a la historia clínica electrónica, siendo los encargados de mantener y mejorar tanto el hardware como el software para la implementación de la historia clínica electrónica. No puede decirse que sea infrecuente en el marco de los hospitales y centros de salud encontrar un ordenador en el que un usuario anterior ha dejado su sesión abierta, de manera que, durante un lapso de tiempo más o menos prolongado hasta que la sesión se bloquea, cualquier otro usuario tiene la oportunidad de acceder a las historias clínicas a las que el usuario anterior tuviera acceso[18]. Cuanta más gente tenga acceso a los historiales clínicos, el derecho a la protección de datos del paciente se encontrará en mayor peligro. En consecuencia, además del peligro que puede suponer un ataque informático en la red sanitaria, las personas que trabajan en el propio sistema sanitario pueden crear riesgos[19].

Al respecto, el artículo 5 de la LOPGDD recoge que los responsables y encargados del tratamiento de datos así como todas las personas que intervengan en cualquier fase de este estarán sujetos al deber de confidencialidad. Deber que adquiere una enorme relevancia en el ámbito sanitario, por las características de los datos a tratar y porque este deber es uno de los pilares de la especial relación de confianza médico-paciente. Pero este deber se extiende a toda persona que tenga acceso a los mismos, y no únicamente a aquéllas cuya profesión esté específicamente sujeta al deber de secreto

---

[18] SALUD CASANOVA ASENCIO, A., "Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias", *Indret*, Núm.2, 2019, p. 9

[19] El historial clínico electrónico posibilita la venta de datos de los pacientes. Al igual que lo ocurrido en el proyecto VISC+ de la Comunidad Autónoma de Cataluña que ha sido expuesto anteriormente, el Departamento de Salud y Asistencia Social de los últimos gobiernos británicos ha estado vendiendo datos médicos de millones de pacientes del Servicio Nacional de salud no solo a compañías farmacéuticas estadounidenses, sino también a otras multinacionales, y ha engañado a los pacientes asegurando que dicha información estaba anonimizada. Sin embargo, altos cargos del NHS han admitido que los datos relativos a la salud de los pacientes recopilados y vendidos pueden vincularse de forma rutinaria a los historiales clínicos de los pacientes a través de cualquier consulta médica posterior. Véase al respecto: THE GUARDIAN., "Releaved: how drugs giants can access your health records", *The Guardian*, 8 de febrero de 2020, disponible en: https://www.theguardian.com/technology/2020/feb/08/fears-over-sale-anonymous-nhs-patient-data#:~:text=The%20Department%20of%20Health%20and,leading%20experts%20in%20the%20field *[Última consulta: 22 de mayo de 2021]*

profesional, todas las personas que accedan al historial clínico de una persona tendrán el deber de confidencialidad.

2.2.Internet de las cosas en la sanidad:

2.2.1. Concepto:

El concepto de "Internet de los objetos" o "Internet de las cosas" (IdC), traducido del término inglés "*Internet of Things"* (IoT), se refiere a una infraestructura en la que miles de millones de sensores incorporados a dispositivos comunes y cotidianos ("objetos" como tales, u objetos vinculados a otros objetos o individuos) registran, someten a tratamiento, almacenan y transfieren datos; a su vez, al estar asociados a identificadores únicos, estos objetos interactúan, de forma automática y sin que el usuario lo perciba, con otros dispositivos o sistemas haciendo uso de sus capacidades de conexión en red[20]. La Unión Internacional de Telecomunicaciones ("*International Telecommunication Union"* o ITU) define los IdC como una infraestructura global para la sociedad de la información permitiendo servicios avanzados mediante la interconexión de aparatos (físicos y virtuales), basados en tecnologías de información y comunicación interoperables existentes y en desarrollo[21].

De una forma gráfica puede definirse el IdC como una arquitectura informática que permite que los aparatos conectados a la red compartan información derivada del usuario y de su ambiente. Los elementos esenciales de esta definición son la existencia de una cosa u objeto, la cual comparta información que puede ser personal o no, y la cesión de esa información que se efectúa a través de una red, que puede ser internet u otra distinta[22]. Es importante subrayar que debe existir algún tipo de intercambio de información para que los aparatos trabajen en el mundo real. No se trata únicamente de que un objeto cotidiano como, por ejemplo, un electrodoméstico cuente con un software integrado que recopila información sobre el uso que se efectúa de ese objeto y lo transforme en datos que procesa, además es preciso que dicho aparato envíe la información a una red, lo que lo convierte en parte del mundo del Internet de las cosas[23].

Aunque el término fue creado en el año 1999 en ese momento las redes de telecomunicaciones aún se hallaban en un estado incipiente y era inverosímil pensar que un objeto se pudiera conectar a la red y que transmitiera la información que contenía. Pero, gracias a los avances de la nanotecnología y sus implicaciones en las infraestructuras de red, soportada por redes de cuarta y quinta generación (4G y 5G), que permitieron hacer uso de mayores velocidades de anchos de banda y ubicuidad en la conectividad, esta visión de hiperconectividad se ha empezado a materializar. Los

[20] GT29. Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos, 1471/14/ES (WP 223), 2014, p.4
[21] UIT. Recomendación Y.4000/Y.2060**,** 15 de junio de 2012, p. 8
[22] JERVIS ORTIZ, P., "Internet de las cosas y protección de datos personales", *Revista Chilena de Derecho y Tecnología*, Vol. 4, Núm. 2, 2015, p.10
[23] BARRIO ANDRÉS, M., *Internet de las cosas*, Reus, Madrid, 2018, p. 24

dispositivos han mejorado su capacidad de procesamiento, almacenamiento y transmisión, permitiendo conectar casi cualquier objeto a la red de Internet. Dicha tecnología posee múltiples aplicaciones hasta el punto de que está transformando nuestra cotidianeidad. Así, por ejemplo, hoy se puede obtener información en tiempo real sobre el estado del tráfico de una ciudad, el nivel de combustible de un vehículo, el ritmo cardíaco de un paciente etc.[24]

Para que un dispositivo pueda ser clasificado dentro de la categoría de Internet de las cosas, debe poder llevar a cabo las siguientes cinco operaciones, a saber, percibir el entorno, recolectar los datos, almacenarlos, analizarlos y actuar en base a los mismos, es decir, ser interoperables. Es patente que la interoperabilidad y el Internet de las Cosas están intrínsecamente conectados y se necesitan mutuamente para alcanzar su máximo potencial. Si bien se ha dicho que el valor de cualquier producto de IdC está determinado por un proceso de aprendizaje automático avocado a alimentar la disciplina de la inteligencia artificial[25].

Según los expertos, se pueden diferenciar tres tipos de IdC: las prendas inteligentes, los sensores auto-cuantificadores y la domótica[26]. Las prendas inteligentes o "*wereables*", son objetos y ropa cotidiana como relojes y gafas en los que se incluyen sensores para ampliar sus funciones. En este tipo de soportes, se pueden implantar cámaras, micrófonos y sensores que tienen la capacidad de grabar y guardar los datos en el propio aparato, y eventualmente también de transferir datos al fabricante del dispositivo. Este modelo de dispositivo conectado hace, por tanto, referencia al conjunto de dispositivos electrónicos que se pueden portar en alguna parte del cuerpo, extra o intercutáneamente y que son capaces de obtener, tratar o transferir información interactuando de forma continua con el usuario.

El segundo tipo referido lo constituyen los sensores auto-cuantificadores, los cuales están diseñados para ser portados por personas que deseen registrar información sobre sus propios hábitos y estilos de vida. Se trata de aparatos comercializados para usos personales como en entrenamiento o los hábitos de vida. Por ejemplo, un acelerómetro colocado en el cinturón de un sujeto podría medir los movimientos del abdomen (datos en bruto), extraer información sobre el ritmo de la respiración (datos agregados e información extraída) y mostrar el nivel de estrés del mismo (dato visualizable).

En el tercer tipo de instrumentos conectados se halla la domótica. En efecto, los dispositivos IdC también pueden ser colocados en oficinas u hogares. Suelen estar alojados en aparatos de uso cotidiado, como bombillas, termostatos, detectores de humo, lavadoras u hornos conectados que pueden ser controlados remotamente a través de Internet. Algunos de ellos están dirigidos a monitorizar hábitos o usos de las personas usuarias. Es el caso de los sensores de movimiento que además de tener un uso

[24] GÓMEZ, J.E., "El internet de las cosas oportunidades y desafíos", *Ingeniería e Innovación*, Vol. 5, Núm. 1, 2017, p. 1
[25] GONZÁLEZ OTERO, B. *Interoperabilidad, internet de las cosas y derecho de autor*, Reus, Madrid, 2019, pp. 24-25
[26] GT29. Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos, *cit*., pp. 6-7

de vigilancia del espacio, también pueden detectar la presencia del usuario, analizar cuáles son sus patrones de movimiento y realizar acciones, por ejemplo, encender una luz o alterar la temperatura ambiente.

El Internet de las Cosas ofrece, como se ha puesto de relieve en múltiples ocasiones, nuevas oportunidades a las empresas, ciudadanos y el conjunto de la sociedad, por ello se ha calificado como el elemento clave de Internet del futuro[27]. En concreto, su impacto en el ámbito sanitario es enorme. Mediante el Internet de las Cosas Médicas (IdCM) o "*Internet of Medical Things*" (IoMT)[28], dirigidos a monitorizar la salud de los pacientes, los profesionales sanitarios pueden realizar un seguimiento exhaustivo de los mismos, pero más allá de su uso por el entorno sanitario, estos dispositivos también facilitan que los mismos ciudadanos y sus cuidadores puedan llevar un control sobre su propia salud, dado que les permiten estar informados sobre sus parámetros. Por ejemplo, los dispositivos pueden alertar sobre una caída que ha sufrido una persona, lo cual cobra especial importancia en el caso de las personas mayores. En consecuencia, estos dispositivos ofrecen nuevas oportunidades en el ámbito sanitario tanto a los profesionales sanitarios como a los pacientes y su entorno.

2.2.2. Riesgos que plantea el Internet de las cosas desde la perspectiva del derecho a la protección de datos personales:

La seguridad y la protección de datos personales son relevantes en cualquier sistema, pero más aún en un entorno de IdCM, en el que los datos, que son altamente sensibles, van a viajar desde los sensores hasta los servicios de telemonitorización. Por tanto, es necesario implementar políticas de protección de datos personales adecuadas para lograr un nivel de seguridad adecuado[29].

Aunque el uso de Internet de las cosas plantea distintos riesgos para el derecho a la protección de datos personales del paciente por su frecuencia y gravedad, cabe hacer una mención especial a los ciberataques. Como ejemplo de dicho riesgo, señalaremos los dispositivos cardíacos implantables habilitados para radiofrecuencia de la St. Juse Medical y el transmisor Merlin@home revisados por la Administración de Alimentos y Medicamentos ("*Food and Drug Administration"* o FDA), Agencia del Gobierno de los Estados Unidos, la cual confirmó que debido a las vulnerabilidades que fueron detectadas era posible que un usuario no autorizado, es decir, alguien que no fuese el médico del paciente, accediese de forma remota al dispositivo y modificara sus comandos de programación. En concreto, la Agencia resolvió que, debido a la debilidad

[27] HALLER, S.; KARNOUSKOS, S.; SCHROTH, C., "The internet of things in an enterprise context", en DOMINGUE, J.; FENSEL, D. y TRAVERSO, P. (Eds.), *Future internet symposium*. Springer, Berlin, 2008, p. 14

[28] Cuando se considere que un dispositivo es un producto sanitario, se le aplicará el Reglamento 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios, el cual fue publicado en mayo 2017, entrando en vigor el 26 de mayo de 2020, salvo ciertos artículos.

[29] TRIGO VILASECA, J.D.; SERRANO-ARRIEZU, L.; ASTRAIN ESCOLA, J.J; FALCONE LANAS, F., "Smart Cities, IoT y Salud: Retos de Internet of Medical Things (IoMT)", *I+ S: Revista de la Sociedad Española de Informática y Salud*, Núm. 129, 2018, p. 10

de la seguridad del transmisor era posible que un tercero no autorizado modificara remotamente el ritmo de funcionamiento, agotase la batería del dispositivo cardíaco o administrase descargas[30].

Tal y como se ha expuesto, mediante los ataques cibernéticos, los hackers que logren el acceso a los dispositivos pueden poner en peligro la vida de los pacientes, pero el sector salud también se enfrenta al peligro de los "*ransomware"* o secruestros de datos que sirven principalmente para chantajear a los responsables de los centros sanitarios. Cabe citar entre otros casos, que el 12 de mayo de 2017 se llevó a cabo a escala global el conocido secuestro de datos conocido como "*WannaCry*"[31] que produjo, entre otras incidencias graves, el cambio de ruta de multitud de ambulancias y la cancelación de operaciones programadas[32]. Como consecuencia de este ataque, el Servicio Nacional de Salud de Inglaterra (NHS) tuvo costo añadido de 92 millones de libras.

2.3. Las aplicaciones informáticas en sanidad:

2.3.1. Concepto:

Las aplicaciones móviles, más conocidas como "*app-s*", hacen referencia a cualquier software al que se puede acceder desde un teléfono móvil o dispositivo electrónico inteligente. Las aplicaciones pueden recoger gran cantidad de datos a partir del dispositivo inteligente (datos de ubicación, datos previamente almacenados por el usuario en el dispositivo o datos procedentes de los distintos sensores conectados) y dependiendo de las especificaciones autorizadas por el usuario, pueden además procesar los datos y transmitiros a terceros con fines comerciales o de innovación con el fin de proporcionar servicios nuevos e innovadores al usuario final[33].

Actualmente, existen múltiples aplicaciones móviles para todo tipo de funciones: ocio, deporte, alimentación, salud etc. Asimismo, han surgido aplicaciones móviles destinadas a las personas mayores, cuya finalidad consiste en monitorizar sus rutinas y permitirles llevar una vida más autónoma[34]. El criterio fijado por el sector sanitario para

---

[30] Véase al respecto: FDA. Cybersecurity Vulnerabilities Identified in St. Juse Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication. 9 de enero de 2017, disponible en: https://wayback.archive-it.org/7993/20201222110135/https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-identified-st-jude-medicals-implantable-cardiac-devices-and-merlinhome *[Última consulta: 15 de mayo de 2021]*

[31] Se trata de un software malicioso que bloquea el acceso de los usuarios a los archivos o sistemas, manteniendo los mismos como rehenes hasta que la víctima pague un rescate a cambio de un clave de descifrado que le permite acceder a los archivos o sistemas encriptados por el programa. Véase al respecto: MOHURLE, S. y PATIL, M., "A brief study of wannacry threat: Ransomware attack 2017", *International Journal of Advanced Research in Computer Science*, Vol. 8, Núm. 5, 2017, p. 1938

[32] GHAFUR, S.; KRISTENSEN, S.; HONEYFORD, K.; MARTIN, G.; DARZI, A. y AYLIN, P., "A retrospective impact analysis of the WannaCry cyberattack on the NHS", *NPJ digital medicine*, Vol. 2, Núm. 1, 2019, p. 1

[33] GT29. Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, 00461/13/ES (WP 202), 27 de febrero de 2013**,** p.2

[34] GONZÁLEZ OÑATE, C. y FANJUL PEYRÓ, C., "Aplicaciones móviles para personas mayores: un estudio sobre su estrategia actual", *Aula abierta*, Vol. 47, Núm. 1, 2018, p. 108

la categorización de las aplicaciones médicas no ha sido el público objetivo, sino la finalidad de las mismas. En función de este criterio, se ha establecido una clasificación de las aplicaciones en torno a seis categorías: accesibilidad, vida cotidiana, entretenimiento, comunicación personal, seguridad y salud[35].

Las aplicaciones de accesibilidad son aquellas que se orientan a la conversión del teléfono móvil en un dispositivo accesible o a la utilización del mismo para mejorar la accesibilidad de los mayores, como las apps destinadas a incrementar la visibilidad y legibilidad, los potenciadores de sonido y los lectores de etiquetas para identificar correctamente los productos. Esta última modalidad, por ejemplo, permite a las personas de edad avanzada identificar la medicación que han de tomar.

En la categoría de "vida cotidiana", se encuentran las aplicaciones móviles destinadas a facilitar o mejorar determinados aspectos de la vida de las personas mayores, especialmente de aquellas que viven solas. La mayor parte de las aplicaciones contempladas en esta categoría ofrecen información de interés para los usuarios como actividades sociales y culturales de su entorno. No obstante, existe un segundo tipo de aplicación de organización personal: gestores de tareas, asistentes de compra, economía del hogar etc. también destinados a facilitar la gestión de las tareas cotidianas de las personas mayores.

El tercer tipo de aplicativo citado lo constituyen las de entretenimiento: juegos, revistas o rutas, creadas y adaptadas expresamente a las necesidades de las personas mayores. El entretenimiento constituye la principal finalidad de estas aplicaciones, pero en algunos casos, estas aplicaciones también tienen la finalidad de ejercitar capacidades cognitivas o motoras, por lo que se podría prever una doble catalogación de las mimas.

Las aplicaciones de comunicación personal permiten que las personas mayores puedan comunicarse con su entorno más cercano. También tienen una implicación en el ámbito sanitario, dado que estas personas pueden estar en contacto con sus familiares aunque sea en la distancia, teniendo este acto especial transcendencia en la salud psicológica de los mayores. Por ejemplo, las personas mayores que han dispuesto de aplicaciones que permiten realizar video llamadas en la pandemia, han podido sentirse menos aisladas que aquellas que no disponen de estas tecnologías o no son capaces de hacer uso de ellas.

En la categoría de seguridad, existen tres subgrupos de aplicaciones dirigidas a mejorar la protección de las personas de edad avanzada. Los gestores de cámaras audiovisuales permiten a los familiares seguir el día a día de los mayores cuando están solos. En el subgrupo de emergencia, se sitúan determinadas aplicaciones basadas en un sistema sencillo y directo de interacción, como un único botón de grandes dimensiones, para alertar a familiares y profesionales del cuidado de una necesidad urgente de asistencia. El tercer tipo de aplicaciones de seguridad, son las de localización, que se basan en la

[35] MARTÍNEZ ROLÁN, X. y PIÑERO OTERO, T., "Tipología y funcionalidades de las aplicaciones móviles para mayores. A un tap del envejecimiento activo", *Ámbitos Revista Internacional de Comunicación*, Núm. 29, 2015, pp. 5-7

tecnología de posicionamiento de los teléfonos inteligentes para efectuar el seguimiento o geolocalización de los mayores, especialmente de aquellos aquejados de algún tipo de demencia, indicando el posicionamiento del portador del teléfono en un mapa o enviando de forma automática un mensaje con la ubicación exacta de la persona en cuestión.

Algunos de los anteriores grupos de aplicaciones tienen un efecto directo o indirecto en la salud de este sector poblacional, pudiendo identificarse diversos tipos: los que aportan información para el desarrollo de una vida saludable, las alertas y recordatorios para la dosificación de medicamentos, la agenda de citas médicas, las destinadas a promover el ejercicio físico y/o cognitivo, las de monitorización de la salud o las de cuidado en el hogar. Algunas aplicaciones están enfocadas directamente a la monitorización de ciertas enfermedades como la diabetes. Estas aplicaciones permiten a los pacientes calcular las dosis de hidratos y la administración de insulina permitiendo, a su vez, a los médicos monitorizarlos de forma remota. También existen aplicaciones para el seguimiento de las lesiones de la piel. Gracias al registro fotográfico estas apps posibilitan al usuario realizar un seguimiento de sus manchas cutáneas, siendo herramientas de gran ayuda para la prevención y detección precoz del cáncer de piel, un tipo de cáncer muy común en las personas mayores.

Las aplicaciones móviles introducen un nuevo canal de comunicación médico-paciente a distancia (*online*), dejando atrás el clásico canal de comunicación presencial médico-paciente (*off line*). Además, los aplicativos citados permiten al paciente registrar sus síntomas (dolor, fatiga, etc.) y sus constantes vitales (tensión arterial o frecuencia cardíaca) de forma periódica y desde cualquier lugar. Por tanto, las aplicaciones móviles constituyen una fuente para el autoconocimiento, posibilitando que el paciente de edad avanzada se responsabilice de su tratamiento, mejorando la adherencia a los tratamientos y promoviendo hábitos de vida más saludables[36].

2.3.2. Riesgos que plantean las aplicaciones informáticas desde la perspectiva de la protección de datos personales:

Las aplicaciones informáticas a las que hemos aludido en el párrafo anterior plantean numerosos riesgos desde la perspectiva de la protección de datos personales del usuario. Según indicó la Agencia Española de Protección de Datos (AEPD), existe un importante riesgo de violación del derecho a la protección de datos al proporcionar datos de salud a aplicaciones, aunque en ellas se indique que esos datos estarán disociados. Asimismo, en ciertas aplicaciones no aparece detallada la política de privacidad y tampoco se indican los fines para los que van a usarse esos datos personales ni quién va a acceder a

[36] LARRUCEA RODRIGO, C., "Mhealth y Bigdata en sanidad", Blog Derecho y salud no van siempre de la mano, 14 de abril de 2016, disponible en: https://carmenrodrigodelarrucea.wordpress.com/2016/04/14/mhealth-y-bigdata-en-sanidad/ *[Última consulta: 15 de mayo de 2021]*

los mismos[37]. Por su parte, en palabras del Grupo de Trabajo del artículo 29 (GT29), los principales riesgos de las aplicaciones de salud son la falta de transparencia y la falta de conocimiento por parte del usuario de los tipos de tratamiento de datos que las aplicaciones pueden realizar. Por otra parte, existe en la mayor parte de los casos una tendencia hacia la maximización de colecta de datos aun cuando no sean necesarios desde el punto de vista de la finalidad enunciada. También se han puesto de manifiesto las insuficiencias de las medidas de seguridad y dispersión de los numerosos agentes que intervienen en el desarrollo de aplicaciones[38].

Para poder utilizar estas aplicaciones se ha de realizar un contrato de uso de software, en el cual el propietario del software (licenciante) concede una licencia o autorización de uso al usuario (licenciatario) de forma gratuita o a cambio del pago de un precio**.** De esta forma, el usuario puede utilizar el software sin que se le transfiera la propiedad intelectual del mismo[39].

Al instalar la aplicación, marcando la meritada casilla de "he leído y acepto", el usuario acepta las condiciones estipuladas en la misma, quedando obligado por los términos de dicho contrato. Las condiciones para los usuarios finales, las personas que van a utilizar de manera directa un producto de software, son aquellas que se aceptan como paso previo para que dicha aplicación sea operativa en el dispositivo móvil, en consecuencia, es muy importante que el usuario lea la licencia para conocer sus condiciones de uso, y así valorar si realmente quiere instalar o no la aplicación.

Cuando se instala una aplicación, se concede una serie de permisos que pueden ser realmente peligrosos de cara a la protección de datos del usuario, y generalmente, no se presta atención a la transcendencia de los mismos. Entre los permisos más usuales, se encuentran los siguientes: el relativo al calendario, que puede usarse para controlar a un usuario, dado que se podrá conocer la actividad que está realizando; contactos, a los que se puede acceder en el caso de permitirlo el usuario; a la cámara, a la app se le permite tomar fotos y grabar vídeos por sí misma; memoria, se permite el acceso ya sea a un sistema de almacenamiento externo como la tarjeta SD o al almacenamiento interno del propio dispositivo, autorizando al dispositivo a acceder al contenido o incluso a que almacene archivos; micrófono, se autoriza que se graben las conversaciones telefónicas o incluso que los micrófonos actúen como espías en cualquier momento[40]; a los mensajes, se permite que la aplicación pueda acceder a la

[37] AEPD., "Comunicado en relación con webs y apps que ofrecen autoevaluaciones y consejos sobre el Coronavirus", 16 de marzo de 2020, disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-de-la-aepd-en-relacion-con-webs-y-apps-que-ofrecen *[Última consulta: 15 de mayo de 2021]*

[38] GT29. Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, *cit.*, pp. 6-7.

[39] GOITIA FUERTES, M., *Aplicaciones informáticas de administración de recursos humanos*. Ediciones Paraninfo, Madrid, 2015, pp. 4-5

[40] Cabe recordar el caso de la Liga de Fútbol, en el cual se usaron los micrófonos de los teléfonos de millones de aficionados para espiar a los bares que ponían partidos y así detectar posibles fraudes. Véase al respecto: SÁNCHEZ, J.L., "La liga de futbol usa el micrófono del teléfono de millones de aficionados para espiar a los bares", *El Diario*, 10 de junio de 2018, disponible en: https://www.eldiario.es/tecnologia/Liga-Futbol-microfono-telefono-aficionados_0_780772124.html *[Última consulta: 15 de mayo de 2021]*

mensajería del teléfono; a la ubicación, gracias a esta autorización, la app puede saber en qué lugar se encuentra en todo momento el usuario; a las propiedades del teléfono, se autoriza a que se sepan todas las características del teléfono móvil del usuario (número, estado de la red…)[41].

Las aplicaciones móviles de sanidad hacen que los usuarios sean más conscientes de su estado de salud, llegando a fomentar la autonomía los usuarios, en especial, la autonomía de las personas mayores, pero es imprescindible garantizar que estas puedan utilizar las aplicaciones con completa seguridad, respetando en todo momento su derecho a la protección de datos. Existen numerosas aplicaciones de dudosa fiabilidad y muchos usuarios no saben identificar cuáles son las aplicaciones que realmente respetan la normativa de protección de datos personales.

En muchas ocasiones, las aplicaciones presentan debilidades técnicas relacionadas con una funcionalidad no ajustada a lo publicitado, cálculos erróneos, deficiencias técnicas, información incompleta y/o incorrecta, etc. También pueden proporcionar una falsa sensación de seguridad que limite la adopción de medidas urgentes dirigidas por un facultativo, por ejemplo, si una aplicación de ayuda al diagnóstico precoz de una enfermedad grave da un falso negativo, puede evitar que se adopten medidas inmediatas. Por ello, es necesario que los usuarios cuenten con fuentes transparentes de información sobre su calidad para decidir cuál es la aplicación más apropiada para sus necesidades.

Pero la seguridad en el campo de la salud no solo se restringe a la evitación de daños físicos, sino que cobra especial relevancia la salvaguarda de la integridad y confidencialidad de la información personal sanitaria involucrada[42]. Unas medidas de seguridad insuficientes pueden provocar el tratamiento no autorizado de información personal sensible cuando, por ejemplo, un desarrollador de aplicaciones sufre una violación de datos personales o si la propia aplicación permite filtraciones de datos personales[43].

La complejidad que reviste el desarrollo de las apps hace que se multipliques los agentes que intervienen en las mismas, lo que también supone un riesgo grave para la protección de datos. Entre los citados agentes podemos incluir: desarrolladores de aplicaciones, propietarios de aplicaciones, tiendas de aplicaciones, fabricantes de sistemas operativos y de dispositivos, y otras terceras partes que pueden intervenir en la recogida y el tratamiento de datos personales a partir de dispositivos inteligentes, como proveedores de análisis y publicitarios.

---

[41] CORCOBADO, M.A., "Estos son los permisos que concedes cuando instalas una app", *El País*, 31 de marzo de 2017, disponible en: https://elpais.com/tecnologia/2017/03/27/actualidad/1490626770_125439.html *[Última consulta: 15 de mayo de 2021]*

[42] SALIDO, J.; DÉNIZ, O. Y BUENO, G., **"**Especial m-health (salud móvil): Desarrollo de aplicaciones de salud para dispositivos móviles", *Sociedad Española de Informática y Salud*, Núm.110, 2015, p. 12

[43] GT29. Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, *cit.***,** p. 8

Es evidente, por tanto, que para alcanzar el nivel adecuado de privacidad y protección de datos, deben colaborar todas las partes del ecosistema de las aplicaciones. Esto es especialmente importante por lo que se refiere a la seguridad, materia en la que sea ha dicho que "la cadena de agentes solo puede ser tan fuerte como su eslabón más débil"[44].

Por otra parte, las aplicaciones pueden almacenar los datos en el terminal del usuario y también almacenarlos en un servidor remoto a través de un servicio de almacenamiento en la nube. Para evitar riesgos de accesos no autorizados a la información es necesario determinar las medidas de seguridad a implementar por parte de cada uno de los distintos intervinientes en el proceso de desarrollo, puesta en marcha y mantenimiento de la misma, para evitar accesos no autorizados a la información[45].

A su vez, las aplicaciones, han de ser acreditadas por un organismo que garantice su calidad y seguridad. Si no se ha realizado dicha acreditación, el usuario se encuentra ante potenciales amenazas de seguridad, y en el caso de las aplicaciones médicas, pueden crearse riesgos para la salud del paciente[46].

2.4.Big Data en la sanidad:

2.4.1. Concepto:

El término Big Data designa la actividad de tratamiento de grandes volúmenes de datos anónimos o nominativos. Este fenómeno comprende la capacidad tecnológica para recoger y tratar grandes volúmenes de datos para luego extraer nuevos conocimientos de los mismos[47]. Es un anglicismo plenamente aceptado e integrado, traduciéndose asimismo como "tratamiento masivo de datos". Se creó en los años 80, cuando los procesadores y la memoria computacional hicieron posible analizar más información. Sin embargo, no deja de ser el último paso de la humanidad en un camino ancestral: el deseo de comprender y cuantificar el mundo[48].

---

[44] Ibid., p. 2

[45] PUYOL, J. "El régimen legal de las apps", *confilegal*, 2 de marzo de 2016, disponible en: https://confilegal.com/20150420-el-regimen-legal-de-las-apps/ *[Última consulta: 20 de mayo de 2021]*

[46]La Agencia de Calidad Sanitaria de Andalucía otorga el Distintivo "AppSaludable". Este distintivo reconoce la calidad y seguridad de las apps de salud. Aquellas apps de salud que superen el proceso de validación, llevado a cabo desde la Agencia de Calidad Sanitaria de Andalucía, obtendrán el Distintivo AppSaludable, y formarán parte de un directorio de apps destacadas por su calidad y seguridad. Este distintivo se basa en las 31 recomendaciones publicadas en la "guía de recomendaciones para el diseño, uso y evaluación de apps de salud", que se estructuran en 4 bloques: diseño y pertinencia, calidad y seguridad de la información, prestación de servicios y confidencialidad y privacidad. Véase al respecto: JUNTA DE ANDALUCIA., "Distintivo AppSaludable", *calidadappsalud*, disponible en: http://www.calidadappsalud.com/distintivo-appsaludable/ *[Última consulta: 17 de mayo de 2021]*

[47] CdE. Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data, 23 de enero de 2017, p. 2

[48] GIL GONZÁLEZ, E., *Big data, privacidad y protección de datos*, Imprenta Nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2016, p. 19

El fenómeno hace referencia a dos cuestiones íntimamente relacionadas, en primer lugar, a la gran cantidad de datos disponibles, que pueden ser utilizados con diversos fines por parte de las empresas, estados y particulares. En segundo lugar, el conjunto de tecnologías cuyo objetivo es tratar grandes cantidades de datos empleando complejos algoritmos y estadística con la finalidad de hacer predicciones, extraer información oculta o correlaciones imprevistas para propiciar la toma de decisiones. Dada esta cantidad de datos, los mismos no pueden ser tratados de manera convencional ya que superan los límites y capacidades de las herramientas de software habitualmente utilizadas para la captura, gestión y procesamiento de datos[49]. Se refiere tanto a los propios datos como a su análisis[50].

Respecto a su objetivo, al igual que los sistemas analíticos convencionales, consiste en convertir el dato en información que facilita la toma de decisiones, incluso en tiempo real. Es decir, aportar y descubrir un conocimiento oculto a partir de grandes volúmenes de datos[51]. Las empresas lo utilizan para entender el perfil, las necesidades de sus clientes respecto a los productos y/o servicios vendidos, lo cual les permite adecuar su modelo de negocio, pero también se utiliza en el ámbito sanitario.

Los tres elementos, conocidos como las tres "uves" de las bases de datos (volumen, variedad y velocidad), eran incompatibles años atrás creando una tensión que obligaba a elegir entre ellas. Se podía analizar un gran volumen de datos y a alta velocidad, pero era necesario que fueran datos sencillos, por ejemplo, datos estructurados en tablas. Alternativamente, se podían analizar grandes volúmenes de datos muy variados, pero no a gran velocidad. Para poder procesar un gran volumen de datos era necesario dejar que los sistemas trabajaran durante horas o incluso días. Sin embargo, con la aparición del fenómeno Big Data desapareció la necesidad de elegir entre las tres uves. Posteriormente, a estas tres "uves" se les añadieron dos más: la veracidad y el valor[52].

El concepto del volumen o cantidad de los datos procesados por ordenadores cada vez más potentes se encuentra en una continua evolución, ya que los avances tecnológicos permiten tratamientos de volúmenes cada vez más grandes. Si se habla de grandes magnitudes se refiere a tratamientos de "*Terabytes*" o "*Petabytes*". El concepto de volumen es muy variable y cada día que pasa eleva lo que se puede considerar como "grandes volúmenes de datos". Respecto a la variedad, se refiere a la introducción de otros tipos de de datos que no se utilizan de forma convencional. En cuanto a la velocidad, se trata de la rapidez con la que los datos se recopilan, procesan y se toman decisiones a partir de ellos. La velocidad a la que se crean y procesan los datos está en continuo aumento, y con frecuencia para las organizaciones es importante poder

[49] CÁRCAR BENITO, J.E. "El Big Data en la organización sanitaria: nuevos tiempos y nuevos cambios", Blog Federación Española de Sociología (FES), disponible en: https://docplayer.es/41738879-El-big-data-en-la-organizacion-sanitaria-nuevos-tiempos-y-nuevos-cambios-un-estudio-previo.html *[Última consulta: 2 de mayo de 2021]*

[50] CdE. *Manual de legislación europea de protección de datos*, Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2018, p. 394

[51] PUYOL, J., "Una aproximación a big data", *Revista de Derecho de la Universidad Nacional de Educación a Distancia (UNED),* Núm.14, 2014, p. 485

[52] GIL GONZÁLEZ, E., *Big data, privacidad y protección de datos, cit.* p. 20

analizarlos de forma muy rápida, incluso en tiempo real. El concepto de la veracidad hace alusión a la fiabilidad de los datos, extraer datos de calidad eliminado la imprevisibilidad inherente de algunos, para de esta forma, llegar a una correcta toma de decisiones[53]. Esto es, hace referencia al nivel de fiabilidad o de calidad de los datos. Finalmente, el valor trata de la importancia del dato para el servicio o el negocio.

La sociedad actual se encuentra inmersa en la era de la información, donde se dispone de grandes cantidades de datos, lo que da como resultado un enorme volumen de datos. Estos datos llegan a gran velocidad y requieren procesamiento en tiempo real. Pueden encontrarse en muchos formatos, como datos estructurados, semiestructurados o no estructurados, lo que implica variedad. Estos datos han de ser "purificados" para mantener la veracidad. Finalmente, deben aportar valor[54].

Como se ha referido más arriba, mediante la organización de los datos recolectados se obtiene información, analizando esta información se consigue el conocimiento, y gracias a este conocimiento las organizaciones o empresas pueden tomar decisiones más acertadas y dirigidas a sus usuarios. Se trata de un nuevo mercado en el que los datos son una especie de nueva materia prima. Dado el valor intrínseco de los datos, actualmente se asiste a una transición hacia la monetización que comporta extraer un nuevo valor de los datos y rentabilizarlos, tanto desde el interés privado como el público, o una combinación de ambos. No obstante, la apuesta por la innovación no puede olvidar los aspectos éticos y los derechos fundamentales de las personas, ni la protección de los ciudadanos en el contexto de estos nuevos avances de las tecnologías. Se trata de examinar esta situación para proponer un nivel de protección firme y, por ello, un nivel más avanzado de innovación en este ámbito[55]. Se puede concluir que la recolección de grandes conjuntos de datos y su posterior análisis tiene un impacto directo en el conjunto de derechos que garantizan la privacidad de las personas y generan nuevas preocupaciones a las que el derecho debe hacer frente. Las tareas de garantizar la seguridad de los datos y la protección de la privacidad se vuelven más difíciles cuando la información se multiplica y se comparte cada vez más ampliamente en todo el mundo[56].

En cuanto a la aplicación del Big Data en el modelo sanitario y en general el sector de la salud representa uno de los sectores donde el Big Data está teniendo mayor impacto y donde se prevé que sus aplicaciones pueden experimentar un mayor crecimiento, sobre todo en las áreas de análisis de datos (historias médicas, análisis clínicos…), en la

[53] CÁRCAR BENITO, J.E., "El Big Data en la organización sanitaria: nuevos tiempos y nuevos cambios. Un estudio previo", *docplayer*, disponible en: https://docplayer.es/41738879-El-big-data-en-la-organizacion-sanitaria-nuevos-tiempos-y-nuevos-cambios-un-estudio-previo.html *[Última consulta: 5 de mayo de 2021]*

[54] LUENGO, J.; GARCÍA-GIL, D.; RAMÍREZ-GALLEGO, S.; GARCÍA, S. y HERRERA, F., *Big Data Preprocessing: Enabling Smart Data*, Springer, Gewerbestrasse, 2020, p.1

[55] *LLÁCER, M.R.*; *CASADO, M.* y *BUISÁN, L. Documento sobre bioética y big data de salud: explotación comercialización de los datos de los usuarios de la sanidad pública*, Publicación de la Universidad de Barcelona, Barcelona, 2015, p. 33

[56] GARRIGA DOMÍNGUEZ, A. *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, Dykinson, Madrid, 2016, p. 35

gestión de centros de salud, en la administración hospitalaria, en la documentación científica (generación, almacenamiento y explotación) etc. Los profesionales sanitarios son cada vez más conscientes del cambio de paradigma que supone el Big Data en la práctica de la medicina. Los pacientes, las clínicas y los hospitales detentan grandes cantidades de datos clínicos, tanto en soporte papel como, cada vez más frecuentemente, en formatos electrónicos pero esta información sigue sin poder utilizarse por la dificultad e imposibilidad material de "digerirlos" de forma efectiva, pero si se le hace frente a esta dificultad se abre un horizonte nuevo para el sector sanitario. La investigación en salud si logra asimilar una gran cantidad de datos, tanto estructurados como no estructurados, y los organiza para conseguir comprender mejor las enfermedades que padece la sociedad. Debido a la gran cantidad de datos, se pueden predecir las enfermedades que pueda sufrir la población[57] e igualmente se puede analizar la idoneidad de un tratamiento, lo cual convierte a la medicina personalizada en la llave del futuro.

Otra de las grandes ventajas que representa el Big Data en el ámbito de la salud es que tiene la capacidad, mediante el almacenamiento y análisis de diversas fuentes de información, de llegar a conclusiones y así responder a las preguntas iniciales de los investigadores gracias a la "*real world evidence"* o "evidencia del mundo real". Este sistema permite comprobar en el mundo real la eficacia, por ejemplo, de un medicamento teniendo en cuenta todos los casos de los pacientes que tengan una determinada patología[58]. Complementa eficazmente los ensayos clínicos controlados realizados por los laboratorios para determinar la seguridad y eficacia de un nuevo fármaco y está llamado a sustituir numerosos ensayos reduciendo así el riesgo que suponen para los pacientes voluntarios.

En suma, el Big Data está llamado ha revolucionar el ámbito de la sanidad, mejorando los recursos y evitando las que se produzcan duplicidades de las pruebas. Aunque en un principio suponga una importante inversión para su desarrollo, tras su implementación suponen un gran ahorro.

---

[57] El esquema de la trayectoria de las enfermedades de Dinamarca es un ejemplo de las posibilidades que otorga la aplicación del Big Data en la sanidad. Entre los años 1996-2010 se registraron 6,2 millones de historias clínicas, con un total de 65 millones de encuentros clínicos totales, que comprenden 16 millones de casos de pacientes hospitalizados, 35 millones de casos de clínicas ambulatorias y 14 millones de casos de emergencias. A partir de estos datos, se encontraron 1.171 trayectorias que tienen una fuerte direccionalidad temporal, significado estadístico y, por lo tanto, brindan una imagen global de las enfermedades más comunes. Gracias a la aplicación del Big Data, se logró identificar los patrones de las enfermedades más comunes de la población como la enfermedad pulmonar obstructiva crónica EPOC. El objetivo de este estudio era identificar y caracterizar las trayectorias de las diversas enfermedades utilizando todos los datos recolectados de la población. Véase al respecto: BOECK JENSEN, A.; MOSELEY, P.L.; OPREA, T.I.; GADE ELLESØE, S.; ERIKSSON, R.; SCHMOCK, H.; BJØDSTRUP JENSEN, P.; JUHL JENSEN, L. y BRUNAK, S., "Temporal disease trajectories condensed from population-wide registry data covering 6.2 million patients", *Nature communications*, Vol. 5, Núm. 4022, 2014

[58] CHEW, S.Y; S KOH, M.; MIN LOO, C.; THUMBOO, J.; SHANTAKUMAR, S. y MATCHAR, D. "Making clinical practice guidelines pragmatic: how big data and real world evidence can close the gap". *Ann Acad Med Singapore*, Vol. 47, Núm. 12, 2018, p. 523

2.4.2. Riesgos que plantea el Big Data desde la perspectiva del derecho a la protección de datos:

Frente a las posibilidades que otorga el Big Data en el ámbito sanitario, también es preciso mencionar los riesgos desde la perspectiva del derecho a la protección de datos. El primer riesgo que ha de ser analizado es el del uso de datos nominativos o no anonimizados. Para realizar la anonimización de los datos, se han de eliminar aquellos rasgos susceptibles de identificar a un individuo de forma directa o indirecta. El problema radica en que actualmente mediante técnicas de ingeniería informática es posible en muchas ocasiones reidentificar los datos ligándolos a la persona a quien pertenecen. En casi todos los casos, se puede conseguir la re-identificación si se tiene la voluntad (por razones económicas, empresariales, delictivas...), los conocimientos y los medios técnicos para ello[59]. En el caso de los datos relativos a la salud, a los cuales nos referiremos más adelante, es fácil encontrar esa motivación y los recursos para poder hacerlo y, por lo tanto, cabe cuestionarse la validez de las iniciativas de intercambio de datos sensibles que estén basadas en técnicas de anonimización[60].

Por otra parte, existen desafíos tecnológicos debido a que la mayor parte de los sistemas tecnológicos no están preparados para abordar proyectos de Big Data, destacando la falta de capacidad de almacenamiento de la información o la energía que consumen los grandes centros de computación. La información que procesan los "almacenes de datos" ("*Data Warehouse"*), es información estructurada que ha pasado por numerosos filtros de calidad para poder garantizar que la información de salida tiene una precisión y una exactitud determinada. Sin embargo, cuando se habla de Big Data se hace referencia a la información que puede estar semiestructurada o incluso no tener ninguna estructuración. Por ello, para poder realizar la gestión de esta información desestructurada se precisa de

[59] Entre los problemas del programa público de analítica para la investigación y la innovación en salud, más conocido como "PADRIS", de la Comunidad Autónoma de Cataluña se identifica precisamente la posibilidad de reidentificar al usuario. El presente programa es una adaptación de una propuesta anterior llamada VISC+, una especie de juego de palabras, dado que "visc" en catalán significa "vivo", aunque sus iniciales responden al nombre "*Valorització d'Informació del Sistema Sanitari Català*" (Valorización de Información del Sistema Público de Salud de Cataluña). Con este nombre se trataba de dar una imagen positiva del plan mediante la sugerencia de que las personas podrían llegar a vivir más o mejor gracias al mismo. El objetivo del programa VISC+, al igual que en el programa PADRIS, radica en integrar los datos sanitarios de los historiales clínicos de los ciudadanos en una especie de base de datos común, para ponerlos a disposición de la comunidad científica. Los datos son objeto de un primer uso cuando el paciente accede al servicio de salud, recibe la atención médica, y su información queda almacenada en el sistema. Una vez que la prestación del servicio médico ya ha tenido lugar, los datos quedan guardados de modo pasivo, sin que se siga extrayendo ninguna utilidad de ellos. La propuesta de reutilizarlos parte de la premisa de que es posible y conveniente un uso ulterior, al que se podría llamar "uso secundario", en lugar de que los datos de salud se queden abandonados en un cajón o en un fichero, cobran nueva vida mediante su integración en el Big Data. El proyecto VISC+ ha creado mucha polémica, ha sido criticado por la posibilidad de que las autoridades de salud pública vendan los datos del sistema de salud obtenidos para hacer negocio con ello. El problema más grande que se identifica en el presente proyecto es la posibilidad de re-identificación de los interesados. Aunque el proyecto PADRIS trata de reducir dicho riesgo mediante la anonimización, la efectividad de la presente medida puede ser cuestionable. Véase al respecto: RUDA GONZÁLEZ, A. "Sé lo que hicisteis el último verano. Implicaciones ético-jurídicas del programa de Big Data de Salud en Cataluña a la luz del Reglamento Europeo de Protección de datos", *Papeles el tiempo de los derechos*, Núm. 29, 2018, pp. 4-6

[60] LLÁCER, M.R.; CASADO, M. *y* BUISÁN, L., *Documento sobre bioética y big data de salud: explotación comercialización de los datos de los usuarios de la sanidad pública, cit.* p. 35

una tecnología más avanzada. Las organizaciones pueden utilizar sus propios servidores o la "nube" para almacenar los datos, y este espacio de datos ha de tener una infraestructura que imposibilite todo acceso no autorizado. En el caso de que no cuente con estos requisitos técnicos, podrá existir un riesgo de seguridad.

El tercer riesgo del Big Data desde la perspectiva del derecho a la protección de datos es el perfilado ("*profiling*") y la discriminación como resultado de dicho perfilado. El perfilado es un fenómeno muy extendido y con contenidos de naturaleza variada (listas de infracciones administrativas, de negligencias cometidas en el ámbito profesional, de carácter ideológico o sobre comportamientos políticos, sobre índices de peligrosidad de los individuos, sobre informaciones genéticas, etc.). La inclusión en alguna de estas listas implica, generalmente, consecuencias adversas y perjudiciales para las personas incluidas en las mismas, por ejemplo, situaciones de discriminación por no permitir el acceso a un determinado bien o servicio. El perfilado de la tecnología de tratamiento de datos personales supone claros peligros para la libertad, para el derecho a no ser discriminado y para la propia dignidad personal[61].

La tecnología genera un ranking dentro de la población teniendo en cuenta diversos datos (estudios, situación laboral, enfermedades…) y otorga una puntuación a cada persona, esto es, lo posiciona dentro de un ranking. Cuanto más avance la tecnología y permita que los diversos algoritmos interactúen entre ellos, tras la suma de toda la puntuación obtenida se crearán diversas categorías sociales, y las personas que se encuentren en la categoría inferior podrán ser objeto de un trato discriminatorio que las perjudique. Por ejemplo, el individuo que sea clasificado en la categoría inferior debido a, entre otras cuestiones, su estado de salud, podrá sufrir un trato discriminatorio en el campo de la salud o en el financiero[62].

---

[61] GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua*, *cit.* pp. 70-71

[62] En este sentido, el sistema escocés de "Pacientes escoceses en riesgo de readmisión y admisión", más conocido como SPARRA ("*Scottish Patients At Risk of Readmision and Admisión*"), puede ser un ejemplo de cómo el uso del Big Data puede crear perfiles y discriminar a las personas. El sistema SPARRA es una herramienta que predice el riesgo que tienen los individuos de ser ingresados en el hospital en el plazo de los doce próximos meses. Fue creado en el año 2006 y en sus comienzos solo se aplicaba a personas mayores de 65 años, extendiendo su aplicación a todas las edades en el año 2008. Con los datos de los historiales clínicos de los ciudadanos y el Big Data se identifican los factores que influyen en la hospitalización para después proceder a la predicción del riesgo de hospitalización de los ciudadanos escoceses. Actualmente, más del 80% de los ciudadanos han sido categorizados en un grupo según su riesgo de hospitalización. Esta agrupación permite a los médicos o trabajadores sociales diseñar un plan de acción preventiva para los grupos con mayor probabilidad de riesgo. No obstante, esta misma posibilidad puede crear un riesgo desde la perspectiva del derecho a la protección de datos, puesto que las personas pueden ser objeto de discriminación según el grupo al que pertenezcan. Véase al respecto: NHS. "Scottish Patients at Risk of Readmission and Admission (SPARRA). Developing Risk Prediction to Support Preventative and Anticipatory Care in Scotland", Health and Social Care Information Programme, 2011, p. 4. Disponible en: https://www.isdscotland.org/Health-Topics/Health-and-Social-Community-Care/SPARRA/2012-02-09-SPARRA-Version-3.pdf

En cuarto lugar, se encuentra la contradicción del funcionamiento del Big Data y el principio de minimización de datos. El artículo 5 del RGPD recoge los principios que tiene que cumplir cualquier tratamiento de datos personales. En el apartado 1.c) del citado artículo se recoge el principio de minimización de datos, que exige que los datos que se vayan a tratar sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. El artículo 25.2 del mismo cuerpo legal recoge que el responsable del tratamiento[63] aplicará las medidas técnicas y organizativas apropiadas para garantizar que solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Por tanto, puede afirmarse que el principio de minimización de datos y la base del funcionamiento del Big Data son contradictorios.

2.5.Cloud Computing en sanidad:

2.5.1. Concepto:

El término "*Cloud Computing"* procede de los términos "*Cloud*" (nube), que es el grafismo habitual que se usa para representar Internet, y "*Computing*" (computación), que se podría considerar que reúne conceptos como informática y almacenamiento[64]. Según la definición del Instituto Nacional para los Estándares y la Tecnología de Estados Unidos, más conocido como "NIST" ("*National Institute of Standards and Technology"*), se trata de un modelo de computación que permite conectar un acceso a la red ubicua bajo demanda a un conjunto de recursos informáticos configurables (a saber, redes, servidores, almacenamiento, aplicaciones y servicios) que pueden ser rápidamente provistos y retirados con poco esfuerzo de gestión o de interacción del proveedor de servicio[65]. Por tanto, el usuario puede acceder según su necesidad y gracias a una red de comunicaciones a recursos como almacenamiento, aplicaciones y servicio, y estos últimos pueden ser nuevamente liberados por el proveedor del servicio poco tiempo.

La nube, como recurso centralizado para la prestación integral de servicios a través de la Red sobre la base de la necesidad y la demanda de los clientes, supone dar a los consumidores, negocios, gobiernos y cualquier usuario, la posibilidad de acceder a enormes recursos informáticos desde cualquier dispositivo y en cualquier lugar en que haya acceso a la red[66]. Antes el límite se encontraba físicamente en el ordenador del usuario, ahora, el ordenador va más allá del propio dispositivo, sumando la red a su composición. La consecuencia directa es la reducción de costes tecnológicos, puesto que para aumentar la potencia de cálculo no es necesario con realizar grandes inversiones en

[63] Artículo 4.7 del RGPD: *"la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento".*
[64] TORRES I VIÑALS, J., *Del cloud computing al big data*, Eureca media, Barcelona, 2012, pp. 8-9,
[65] MELL, P. y GRANCE, T., The NIST definition of Cloud computing: Recommendations of the National institute of Standards and Technology, *National institute of Standards and Technology*, 2011, p.2, disponible en: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf
[66] VILLARINO MARZO, J., *La privacidad en el entorno del cloud computing*, Reus, Madrid, 2018, p. 25

hardware sino que será suficiente con conectarse a la nube en lugar de instalar el software en cada equipo[67].

Se distinguen cuatro tipos o modelos de Cloud Computing: el público, el privado, el híbrido y el modelo de comunidad[68]. El público se define como aquel modelo en el cual los servicios e infraestructuras tecnológicas son provistos "*off-site*" o "fuera del sitio" y sobre Internet. Se refiere al almacenamiento externo de los datos en una instalación independiente a la misma empresa, organización, hospital… vía Internet. Será un servicio de nube pública cuando el proveedor de servicios de Cloud proporciona sus recursos de forma abierta a entidades heterogéneas, sin más relación entre sí que haber cerrado un contrato con el mismo proveedor de servicio[69].

El segundo tipo de cloud computing es el privado, modelo de nube en el cual los servicios e infraestructura son provistos y mantenidos dentro de una red privada. Una nube privada es un entorno informático para una organización específica con ventajas de nube pública pero alojado en el centro de datos de una empresa o mediante un proveedor externo. Ofrecen el mayor grado de seguridad, control y gobernabilidad del mercado, pero también requieren que el contratante invierta (parcial o totalmente) en la adquisición de la infraestructura, lo cual reduce los ahorros obtenidos.

El tercero es el híbrido, modelo de nube que incluye una variedad de opciones públicas y privadas con múltiples proveedores y servicios. La dificultad radica en poder controlar de manera eficiente la seguridad en las diferentes plataformas involucradas y garantizar que cada parte del negocio se pueda comunicar con las demás.

Por último, se encuentra el modelo de comunidad, el cual se define como la nube que incluye una variedad de opciones de las nubes públicas o privadas pero pudiendo compartirse entre múltiples proveedores. En este tipo de nubes se ofrecen los servicios en modalidad de comunidad a un colectivo que trabaja para un fin común, como, por ejemplo, proyectos científicos, educativos, etc. y en general para cualquier grupo que necesite una plataforma compartida para un proyecto común. Estas nubes se utilizan cuando dos o más organizaciones forman una alianza para implementar una

[67] Se pueden identificar seis características de esta nueva tecnología: autoservicio, acceso universal, agrupación y reserva de recursos, elasticidad rápida, medible y supervisado, y sencillez. El autoservicio hace referencia a que el consumidor puede usar los servicios en nube conforme a sus necesidades sin ninguna interacción humana con el prestador de servicios. Por otra parte, el acceso universal a la red alude a las capacidades del prestador de servicios las cuales están disponibles en la red y se puede acceder a ellas a través de mecanismos estándar por cualquier cliente, esto es, se puede acceder desde diferentes dispositivos y redes. En cuanto a la agrupación y reserva de recursos, los recursos físicos y no físicos del prestador son asignados y reasignados en función de la demanda de los consumidores. En cuarto lugar, se encuentra la elasticidad rápida, la nube aparece como algo infinito, el usuario puede adquirir más o menos poder de computación como necesite. El servicio es medible y supervisado, los servicios en nube son en todo momento controlados y supervisados por el prestador del servicio. Por último, se ha de destacar que los dispositivos son más sencillos. Ibíd., pp. 27-36

[68] MONTERO MARTÍNEZ, M.A., "Retos y oportunidades del Cloud Computing en la sanidad", *Revista Informática y Salud* (I+S), Núm. 88, 2011, pp. 22-23

[69] AEPD. Guía para clientes que contraten servicios de Cloud Computing, 2018, pp. 6-7

infraestructura de nube orientada a objetivos similares y con un marco de seguridad y privacidad común[70].

El uso de Cloud Computing se está implementando rápidamente en el ámbito sanitario. Esta tecnología permite que los servicios cínicos sean mucho más ágiles, aumentando la eficiencia y eficacia de los recursos sanitarios disponibles, por ejemplo, la nube convierte el acceso a imágenes y diagnósticos en algo inmediato que mejora los niveles de atención a los pacientes[71].

2.5.2. Riesgos que plantea el Cloud Computing desde la perspectiva del derecho a la protección de datos personales:

El riesgo principal de los datos almacenados en la nube consiste en la dificultad de identificar en qué servidor de qué país se están llevando a cabo los tratamientos de datos en tiempo real. Es frecuente que se produzcan fugas de datos y que sea prácticamente imposible trazar a posteriori la cadena de tratamiento que permita identificar al responsable.

Es importante saber dónde se encuentran almacenados físicamente los datos, puesto que la misma naturaleza del servicio de nube informática hace que sea difícil identificar en qué servidor se encuentran. Esta operación es necesario para averiguar si los proveedores están localizados dentro del Espacio Económico Europeo o en países que de una u otra forma garanticen un nivel adecuado de protección de los datos de carácter personal.

Como regla general, se prohíben las transferencias de datos a terceros países salvo que se cumplan los requisitos del capítulo V del RGPD. El Reglamento exige que tanto los responsables como los encargados cumplan los estándares europeos, lo que entraña especiales dificultades de control al tener que valorar varios países para un mismo prestador de servicios. El tratamiento de los datos no siempre se realiza por el encargado, sino que este suele subcontratar a terceros que se pueden localizar en otros países. Estos contratos suelen variar con frecuencia de forma que el proveedor pueda ajustar los recursos que dispone a la necesidad que tiene en cada momento, con el resultado de que sus recursos físicos y virtuales son continuamente reasignados. A pesar de que la normativa de protección de datos prevea duras sanciones por realizar transferencias de datos a terceros países su aplicación es escasa[72].

---

[70] FERNÁNDEZ ALLER, C., "Algunos retos de la protección de datos en la sociedad del conocimiento: especial detenimiento en la computación en nube (Cloud Computing)", *Revista de derecho UNED*, Núm. 10, 2012, p. 134

[71] PEREA MARTÍN, P., "Cloud Computing contribuye a la sostenibilidad del sistema sanitario", *Revista Informática y Salud (I+S)*, Núm. 88, 2011,p. 16

[72] ALKORTA IDIAKEZ, I., "Los riesgos del teletrabajo para la protección de los datos personales de los empleados y de los terceros", en RODRÍGUEZ AYUSO, J.F. y ATIENZA MACÍAS, E. (dir), *El nuevo marco legal del teletrabajo en España: Presente y futuro, una aproximación multidisciplinar*, Wolters Kluwer España, 2021, pp. 24-25

Por este motivo, es especialmente relevante que los servicios de nubes informáticas cumplan el principio de transparencia. Un servicio de Cloud es transparente cuando el contratista puede reclamar información precisa sobre dónde, cuándo y quién ha almacenado o procesado sus datos y en qué condiciones de seguridad se ha producido. Por el contrario, un servicio es opaco cuando el usuario no tiene opción alguna de obtener dicha información[73]. Los clientes no deciden dónde se almacenan sus datos ya que los proveedores no brindan suficiente transparencia, lo cual hace que la falta de control sea una realidad. Los conocidos contratos de adhesión son un gran ejemplo de pérdida de control por parte del cliente, no se le brinda la opción de negociar las cláusulas de dicho contrato, dejando las condiciones por las cuales se desarrollará el tratamiento de todo los datos exclusivamente en manos del proveedor.

De la misma manera, el Cloud Computing fomenta la inseguridad de los datos, posibilitando accesos no autorizados. Por ello, es necesario que el proveedor tome medidas adecuadas para evitar que los hackers accedan a dicha información. Para el funcionamiento de esta tecnología, es indispensable contar con una red, así en el caso de que exista un simple fallo de red no se podrá disponer de los servicios que proporciona el Cloud Computing. Cualquier punto de debilidad en la red, sea en términos de seguridad o en términos de capacidad, implica un riesgo en el primero de los casos y una debilidad en el servicio prestado en el segundo[74].

2.6.Inteligencia artificial en la sanidad:

2.6.1. Concepto:

La inteligencia artificial, también conocida como IA, es una disciplina científica que se ocupa de crear programas informáticos que ejecutan operaciones comparables a las que realiza la mente humana, como el aprendizaje o el razonamiento lógico[75]. Su creación se remonta al año 1943, cuando MCCULLOCH y PITTS crearon el primer modelo de red neuronal artificial, demostrando que el sistema era capaz de aprender y resolver funciones lógicas. En el año 1950 TURING publicó su artículo "*Computing machinery and intelligence*" donde argumentaba que si una máquina puede actuar como un humano puede clasificarse como inteligente. El autor proponía una prueba llamada "Test de Turing", en el cual una persona debía de comunicarse a través de un terminal informático con una entidad (humano o máquina inteligente) que se hallaba en una habitación contigua. Si tras una conversación la persona no era capaz de distinguir si lo que había en la otra habitación era una persona o una máquina, la máquina se consideraría inteligente. La máquina que fuese capaz de pasar el test debía tener

[73] AEPD, Guía para clientes que contraten servicios de Cloud Computing, *cit.*, pp. 9-10
[74] VILLARINO MARZO, J., La privacidad en el entorno del cloud computing, *cit*,. pp. 54-55
[75] RAE. Definición de la inteligencia artificial, disponible en: https://dle.rae.es/inteligencia

reconocimiento del lenguaje natural, razonamiento, aprendizaje y representación del conocimiento[76].

La IA emula algunas de las facultades intelectuales humanas (percepción sensorial como la visión y audición, y su posterior reconocimiento de patrones) en sistemas artificiales[77]. Por su parte, la Comisión Europea lo ha definido como sistemas de software, y posiblemente también hardware, diseñados por humanos para actuar en la dimensión física o digital percibiendo su entorno a través de la adquisición de datos, su interpretación y razonamiento de la información que se derivada de estos datos. Los sistemas de inteligencia artificial pueden usar reglas simbólicas o aprender un modelo numérico, y también pueden adaptar su comportamiento analizando cómo el entorno se ve afectado por sus acciones anteriores[78].

Esta tecnología avanzada se sustenta en algoritmos inteligentes o en algoritmos de aprendizaje que, entre otros fines, se utilizan para identificar tendencias económicas o tratamientos médicos personalizados. Un algoritmo puede ser definido como un conjunto preciso de instrucciones o reglas, o como una serie metódica de pasos que puede utilizarse para hacer cálculos, resolver problemas y tomar decisiones[79]. Gracias a estos algoritmos también se pueden realizar sugerencias y predicciones en áreas como la salud, la educación, el trabajo y el tiempo libre, con todo lo que ello conlleva. Los algoritmos tienen un efecto directo en la vida de cada individuo, pueden predecir sus gustos recomendando canciones, series o películas en base a las antiguas búsquedas y visualizaciones de este, condicionando lo que escucha y ve. Pero también pueden predecir una subida de azúcar de una persona diabética o un ataque epiléptico, llegando a salvar vidas.

Dentro de la inteligencia artificial se distinguen dos conceptos: el aprendizaje automático ("*machine learning*") y el aprendizaje profundo ("*deep learning*"). El primero se refiere al estudio científico de los algoritmos y modelos estadísticos que utilizan los sistemas informáticos para realizar una tarea específica sin estar explícitamente programado[80]. La naturaleza iterativa del aprendizaje automático permite adaptar los métodos a nuevas situaciones y datos[81]. Respecto al aprendizaje profundo, persigue emular el cerebro humano a través de modelos informáticos que funcionan

---

[76] GARCÍA SERRANO, A., *Inteligencia artificial. Fundamentos, práctica y aplicaciones*. RC libros, Madrid, 2012, pp. 2-4

[77] BENÍTEZ, R.; ESCUDERO, G.; KANAAN, S. y MASIP, D., *Inteligencia artificial avanzada*, UOC, Barcelona, 2014, p. 12

[78] THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE., "A definitión of AI: Main capabilities and Disciplines", *ec.europa.eu*, 2019, p. 6, disponible en: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

[79] CORVALÁN, J., "Inteligencia Artificial y derechos humanos". *Diario DPI Cuántico*, Núm. 1, 2017, p. 2

[80] MAHESH, B., "Machine learning algorithms-a review", *International Journal of Science and Research*, Vol. 9, Núm, 2020, p. 381

[81] BHARDWAJ, R.; NAMBIAR, A.R.; DUTTA, D., "A study of machine learning in healthcare". *IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, 2017, p. 237, https://doi.org/10.1109/COMPSAC.2017.164

como un sistema de redes neuronales capaz de analizar los datos. Estas redes neuronales se organizan en capas para reconocer relaciones y patrones complejos en los datos[82], su aplicación requiere un enorme conjunto de información y una potente capacidad de procesamiento[83].

Igualmente, la inteligencia artificial puede ser categorizada como débil ("*narrow artificial intelligente*") o fuerte ("*strong artificial intelligente*"). La inteligencia artificial débil permite diseñar y programar ordenadores de forma que realicen tareas que requieren inteligencia. En cambio, la inteligencia artificial fuerte permite replicar la inteligencia humana mediante máquinas. Esta última implica que un ordenador convenientemente programado no simula una mente, sino que es una mente autoconsciente y por consiguiente debe ser capaz de pensar igual que un ser humano. Sin embargo, la inteligencia artificial débil consiste en construir programas que ayudan al ser humano en sus actividades mentales en lugar de duplicarlas[84].

Los conceptos Big Data e inteligencia artificial están íntimamente relacionados, pero no han de ser confundidos. El Big Data se refiere a la recolección y posterior procesamiento cantidades masivas de datos. Por su parte, la Inteligencia Artificial utiliza algoritmos para crear máquinas capaces de aprender, razonar y tomar decisiones. La Inteligencia Artificial necesita datos para construir su inteligencia, cuanto mayor sea la cantidad de datos a la que acceden los sistemas inteligentes mayor será la posibilidad de aprender de los mismos, pudiendo ofrecer mejores resultados. Se puede decir que el Big Data es el combustible o suministro de la Inteligencia Artificial, esta última puede resolver problemas gracias al almacenamiento masivo y procesamiento de los datos y la posterior aplicación de algoritmos. Dicho de una forma gráfica, el Big Data recoge grandes cantidades de datos y los "limpia", cuando los datos están "limpios" o procesados, entran en juego los algoritmos de la Inteligencia Artificial. Gracias a la capacidad de auto-aprendizaje, la Inteligencia Artificial optimiza los trabajos de Big Data, permitiendo no solo extraer más información sino procesarla más rápidamente y de una forma mejor.

Hoy en día, la inteligencia artificial se aplica en multitud de ámbitos como el financiero, el marketing, la logística y también la sanidad[85]. En el campo de la sanidad, esta tecnología puede diagnosticar enfermedades y proporcionar un tratamiento personalizado, para lo cual se necesita una gran cantidad de datos, de ahí su estrecha relación con el Big Data. En consecuencia, ha de ser comprendido como una ayuda o instrumento para el clínico a la hora de realizar los diagnósticos y tomar decisiones terapéuticas más precisas.

---

[82] CASONATO, C., FASAN, M. y PENASA, S., "Diritto e intelligenza artificiale", *DPCE online*, Núm. 1, 2022, p. 162

[83] ROUHIAINEN, L., *Inteligencia artificial. 101 cosas que debes saber hoy sobre nuestro futuro*, Planeta, Madrid, 2018, p. 22

[84] LÓPEZ DE MÁNTARAS, R., "Algunas reflexiones sobre el presente y futuro de la Inteligencia Artificial", *Novática*, Núm. 234, 2015, pp. 97-98

[85] RUSSELL, S.J. y NORVIG, P., *Inteligencia Artificial: Un Enfoque Moderno*, Pearson Prentice Hall, Madrid, 2004, pp. 32-33

2.6.2. Riesgos que plantea la inteligencia artificial desde la perspectiva de la protección de datos:

Al igual que en el caso del Big Data, existe el riesgo de que la implementada medida de la anonimización no sea real, pudiendo re-identificar al titular de los datos. De la misma manera, se crea el riesgo de elaborar perfiles, discriminando a las personas. El Parlamento Europeo en su resolución de 14 de marzo de 2017[86] hizo hincapié en que como consecuencia de los conjuntos de datos y sistemas de algoritmos que se utilizan al hacer evaluaciones y predicciones en las distintas fases del tratamiento de datos, no solo se pueden realizar violaciones de los derechos fundamentales de los individuos, sino también un tratamiento diferenciado y una discriminación indirecta de grupos de personas con características similares. Para evitar la discriminación que se deriva del perfilado, el Parlamento Europeo instó a la Comisión, a los Estados miembros y a las autoridades encargadas de la protección de datos a que defiendan y adopten las medidas que se impongan para minimizar la discriminación y el sesgo algorítmicos y a que desarrollen un marco ético común sólido para el tratamiento transparente de los datos personales y la toma de decisiones automatizadas.

La citada transparencia se refiere a la opacidad de los algoritmos utilizados. En muchas ocasiones las máquinas terminan siendo una "caja negra" llena de secretos incluso para sus propios desarrolladores, los cuales son incapaces de entender qué camino ha seguido el modelo para llegar a una determinada conclusión. Cuando se juzga a una persona en una sentencia se explica el por qué de la decisión, pero con los algoritmos opacos no se sabe en qué se ha fundamentado la decisión[87]. Estas cajas negras toman decisiones mediante procesos internos incomprensibles para los seres humanos y, además, no son modelos marginales sino de uso generalizado[88]. Las fuerzas y cuerpos de seguridad y las personas afectadas pueden carecer de los medios para comprobar cómo se ha tomado una decisión determinada con ayuda de la inteligencia artificial y, por consiguiente, no podrán saber si se ha respetado la normativa de protección de datos[89].

La Comisión Europea en su Libro Blanco sobre inteligencia artificial recoge que la aplicación de la inteligencia artificial debe considerarse de riesgo elevado en función de lo que esté en juego, y considerando si tanto el sector como el uso previsto suponen riesgos significativos, en especial desde la perspectiva de la protección de la seguridad, los derechos de los consumidores y los derechos fundamentales. De manera más específica, la aplicación de la inteligencia artificial debe considerarse de riesgo elevado

---

[86] PARLAMENTO EUROPEO. Resolución de 14 de marzo de 2017 sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI))

[87] RUBIO, I., "Por qué puede ser peligroso que un algoritmo decida si contratarte o concederte un crédito", El País, 23 de noviembre de 2018, disponible en: https://elpais.com/tecnologia/2018/11/19/actualidad/1542630835_054987.html *[Última consulta: 15 de mayo de 2021]*

[88] CARABANTES, M., "Black-box artificial intelligence: an epistemological and critical analysis", *AI & society*, 2020, Vol. 35, Núm. 2, p. 309

[89] COMISIÓN EUROPEA. Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza, 2020, p. 14

cuando, se emplee en un sector en el que, por las características o actividades que se llevan a cabo normalmente, es previsible que existan riesgos significativos, y cuando la aplicación de la inteligencia artificial en el sector en cuestión se use de manera que puedan surgir riesgos significativos[90]. Así, la aplicación de la inteligencia artificial en este ámbito se considerará generalmente de alto riesgo, puesto que puede crear riesgos significativos para el titular de los datos. La aplicación de los citados dos criterios debe garantizar que el ámbito del marco regulador se adapte a lo necesario y ofrezca seguridad jurídica.

Sin perjuicio de lo anterior, puede defenderse que el mayor riesgo que plantea la inteligencia artificial es la posibilidad de tomar decisiones automatizadas sin la intervención humana. Aunque el valor que otorga al ámbito de la sociedad sea innegable, la inteligencia artificial ha de ser comprendida como una herramienta de apoyo para el profesional sanitario, debiendo existir siempre una intervención humana a la hora de tomar decisiones sanitarias tras el análisis de los datos del interesado.

Para hacer frente a esta situación, el artículo 22 del RGPD, el cual será analizado en profundidad más adelante, prohíbe expresamente la toma de decisiones automatizadas. La prohibición del referido artículo se refiere a las decisiones "basadas únicamente" en el tratamiento automatizado. Para ser considerada como participación humana, el responsable del tratamiento debe garantizar que cualquier supervisión de la decisión sea significativa en vez de ser únicamente un gesto simbólico. La participación debe llevarse a cabo por parte de una persona autorizada y competente para modificar la decisión. Como parte del análisis, debe tener en cuenta todos los datos pertinentes[91].

3. LA SALUD DIGITAL, EL NUEVO PARADIGMA:

3.1.Concepto:

El concepto de la "salud digital", "salud electrónica" o "e-Salud" (traducción del término inglés "*e-Health"*), ha de ser comprendida como el resultado de la aplicación de las herramientas tecnológicas referidas en los epígrafes anteriores al ámbito concreto de la salud. La salud digital constituye un campo emergente que se sitúa en la intersección entre la informática médica, la salud pública y la actividad de las empresas. La salud digital se traduce en nuevos servicios de salud y la información entregada o mejorada a través de Internet y tecnologías relacionadas. El término caracteriza el propio desarrollo técnico, sino también una forma de pensar, una actitud y un compromiso para el pensamiento global en red, para mejorar la atención médica a nivel local, regional y mundial mediante el uso de tecnología de la información y la comunicación global para mejorar la sanidad local, regional y globalmente a través del uso de las tecnologías de la

[90] Ibid., p. 22
[91] GT29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, 6 de febrero de 2018, p. 23

información y la comunicación[92]. El concepto engloba tanto a las nuevas tecnologías como los nuevos modelos de la medicina (la salud móvil y la telemedicina), pero también el aprendizaje y la investigación[93].

Se ha dicho que la salud digital no es una alternativa o mero complemento de la atención sanitaria, sino un nuevo concepto en la prestación del servicio gracias al gran potencial que ofrecen las tecnologías de la información y la comunicación en la mejora del acceso, la reducción de los tiempos de respuesta, la efectividad y contraste de los diagnósticos, y en definitiva, la mejora del servicio al paciente[94]. La salud digital ofrece nuevas oportunidades para mejorar el sistema de salud a nivel local, nacional y global a través de la colaboración y contribución de pacientes, profesionales de la salud, investigadores, instituciones y la industria[95].

El primer elemento que caracteriza a la eSalud es la eficiencia, objetivo de la salud digital que conllevará el ahorro en la asistencia sanitaria. Por ejemplo, a través de las nuevas comunicaciones que existen entre los establecimientos sanitarios y los pacientes, se pretende evitar la duplicidad de las pruebas entre otras cuestiones. Igualmente, se destaca la mejora de la calidad de la atención, aumentar la eficiencia implica no solo reducir los costos, sino al mismo tiempo mejorar la calidad. La salud electrónica puede mejorar la calidad de la atención médica, por ejemplo, al permitir comparaciones entre diferentes proveedores, involucrando a los pacientes como un poder adicional para garantizar la calidad y dirigiendo los flujos de pacientes a los mejores proveedores. La salud digital está basada en la evidencia, su efectividad no debe ser asumida sino probada mediante una rigurosa evaluación científica.

De la misma manera, ha de empoderar a los pacientes, al hacer que las bases de conocimiento de la medicina y los registros electrónicos personales sean accesibles para los pacientes a través de Internet, la salud digital abre nuevas vías para la medicina que se centra en el mismo. En cuanto a la estimulación, se refiere al fomento de una nueva relación entre el paciente y el profesional de la salud, permitiendo que las decisiones se tomen de manera compartida. El sexto elemento es la educación a través de fuentes digitales, se promueve que los pacientes aprendan más sobre la salud y se les facilita información preventiva y personalizada. Por otra parte, la salud digital permite el intercambio de información, se abre la posibilidad de intercambiar la información de manera estandarizada entre establecimientos de salud.

---

[92] EYSENBACH, G., "What is e-health?", *Journal of medical Internet research*, Vol. 3, Núm. 2, 2001, p.1

[93] GADDI, A.; CAPELLO, F. y MANCA, M., *EHealth, Care and Quality of Life,* Springer, Berlin, 2014, p. 17

[94] SAINZ DE ABAJO, B., "M-health y T-health. La evolución natural del E-health", *RevistaeSalud. com*, Vol. 7, Núm. 25, 2011, pp. 2-3

[95] EYSENBACH afirma que la "e" del término "eSalud" no se refiere únicamente a la electrónica, sino que alude a otros diez términos que igualmente empezaban con la letra "e" y permiten entender el término de la salud digital en toda su extensión. Por tanto, la "e" no solo significa "electrónica", sino que implica una serie de otras "e", que juntas definen de una forma más adecuada lo que significa la salud digital. Véase al respecto: EYSENBACH, G., "What is e-health?", *Journal of medical Internet research, cit.,* pp.1-2

El séptimo elemento es la extensión del alcance, lo cual ha de ser comprendido tanto en sentido geográfico como conceptual. La salud digital permite a los consumidores obtener fácilmente servicios de salud en línea de proveedores globales. Por su parte, la ética, implica nuevas formas de interacción médico-paciente y plantea desafíos y amenazas a cuestiones éticas como la práctica profesional en línea y el consentimiento informado. El décimo elemento es la equidad, hacer que la atención médica sea más equitativa es una de las promesas de la salud digital, pero al mismo tiempo existe una amenaza considerable de que la salud electrónica pueda profundizar la brecha las personas que poseen acceso a los ordenadores y las que no pueden costearlo o carecen de las competencias necesarias para usar estas herramientas. Entre la población vulnerables debemos citar a las personas mayores que son las que tienen menos probabilidades de beneficiarse de los avances en la tecnología de la información, a menos que las medidas políticas garanticen un acceso equitativo para todos.

Dado que la salud digital es el término general que abarca tanto la salud móvil como la telemedicina, se analizarán los específicos riesgos que plantean estos dos subgrupos de la e-salud en los siguientes apartados.

3.2.Telemedicina:

3.2.1. Concepto:

Creado en el siglo XIX, el teléfono es considerado como la primera y más simple herramienta de la telemedicina. Más tarde, durante la Primera Guerra Mundial, se establecieron las radiocomunicaciones que fueron ampliamente usadas en las comunicaciones médicas. Sin embargo, la verdadera práctica de la telemedicina empezó en los años cincuenta en los Estados Unidos[96]. La historia de la telemedicina ha estado ligada al desarrollo de las telecomunicaciones, y de esta forma, el telégrafo, el teléfono, la radio, la televisión y los enlaces por satélite han sido utilizados para uso médico desde el primer momento de su creación[97]. Así, la mayor parte de las definiciones clásicas del concepto hacen referencia al ejercicio de la medicina a distancia, el arte de curar no está limitado geográficamente. Por tanto, la idea general es que la telemedicina es una forma más de ejercer la medicina, la cual se práctica para asistir a ciertos pacientes más inaccesibles y así mejorar la calidad de la atención médica[98].

Hace años, se utilizaban indistintamente los conceptos de telemedicina o salud digital, como sinónimos pero no se trata del mismo término. La salud digital se refiere a todas las formas de atención sanitaria electrónica proporcionadas a través de Internet, incluyéndose la información educativa, los productos comerciales, los servicios directos ofrecidos por profesionales etc. La telemedicina se encuentra dentro de la salud digital,

[96] FERRER ROCA, O., *Telemedicina*. Panamericana, Madrid, 2001, p. 2.
[97] MONTEAGUDO, J.L.; SERRANO, L. y HERNÁNDEZ SALVADOR, C., "La telemedicina: ¿ciencia o ficción?", *Anales del sistema sanitario de Navarra*, Vol. 28, Núm.3, 2005, p. 310
[98] LÓPEZ CORONADO, M. y DE LA TORRE, I., *Mejora de la calidad asistencial mediante la telemedicina y la teleasistencia*, Díaz de Santos, Madrid, 2014, p. 949

la primera consiste en la asistencia médica mediante algún medio de comunicación entre dos personas (dos profesionales sanitarios o profesional sanitario y paciente) que no se encuentran situadas en el mismo lugar. Respecto a la segunda, esta se refiere al ámbito sanitario en general que se desarrolla gracias a las TIC. En suma, la telemedicina es su conjunto es salud digital, pero no toda la salud digital es telemedicina. Se pueden diferencias distintos tipos de telemedicina que se agrupan según su especialidad o función.

En el grupo de las especialidades, entre otras, se encuentran las siguientes: telerradiología, la trasmisión electrónica de imágenes radiológicas para realizar una interpretación o consultar un diagnóstico; telecardiología, la transmisión de ruidos cardíacos mediante los estetoscopios digitales acoplados a sistemas telefónicos; teledermatología, el uso de recursos de telemedicina en dermatología mediante la ayuda de la videoconferencia o la transmisión de imágenes, y la telepsiquiatría, la cual se basa generalmente en la utilización de soluciones de videoconferencia que conectan a los pacientes con sus terapeutas[99].

Dentro del segundo grupo destacan las siguientes funciones[100]: teleasistencia, permite la supervisión o la atención urgente del paciente; teleconsulta, puede ser entre diversos profesionales o entre un paciente y un profesional sanitario; telediagnóstico, se refiere al diagnostico realizado a distancia; telemonitorización, permite realizar un seguimiento de algunos parámetros biológicos del paciente; teleformación, sirve para formar a distancia tanto a los profesionales médicos como pacientes en temas relacionados con la salud y la práctica clínica; telerehabilitación, se utiliza para que el paciente pueda realizar sus ejercicios de rehabilitación desde su casa, y la telecirugía, comprendida como la cirugía a distancia empleando recursos telemáticos como la robótica. En los siguientes puntos se analizarán en profundidad la teleasistencia y la telemonitorización por tratarse de dos funciones que cobran especial importancia en el caso de las personas mayores.

3.2.2. Teleasistencia:

a) Concepto:

Tal y como se ha dicho más arriba, dentro de los tipos de telemedicina cobra especial importancia la teleasistencia. Tomemos por ejemplo el Decreto 144/2011, de 28 de junio, del servicio público de teleasistencia[101] del País Vasco, el cual define la teleasistencia como un servicio técnico de apoyo e intervención social, enmarcado en el contexto de los servicios sociales de atención primaria, que permite a las personas usuarias, a través de la línea telefónica y con un equipamiento de comunicaciones e informático específico, disponer de un servicio de atención permanente, las 24 horas del

[99] OPS y OMS., "Marco de implementación de un servicio de telemedicina", 2016, p. 14, disponible en: https://iris.paho.org/bitstream/handle/10665.2/28413/9789275319031_spa.pdf?sequence=6&isAllowed=y
[100] MARTÍNEZ DEL VALLE, M., "Covid-19: más que una pandemia, un cambio en nuestra consulta", *Medicina general y de familia*, Vol. 9, Núm. 4, 2020, p.171
[101] BOPV núm. 124 de 30 de Junio de 2011

día y todos los días del año, atendido por personas específicamente preparadas para dar respuesta adecuada a situaciones de necesidad social o de emergencia[102].

Serán consideradas destinatarias del servicio público de teleasistencia las personas mayores de 65 años que se encuentren en situación de dependencia, reconocida por resolución administrativa del órgano competente o en situación de riesgo de dependencia acreditada mediante dictamen del órgano de valoración de la situación de dependencia. Asimismo, serán destinatarias del presente servicio las personas mayores de 75 años que vivan solas; las personas con discapacidad intelectual en situación de dependencia reconocida por resolución administrativa de órgano competente; las personas con discapacidad física en situación de dependencia reconocida por resolución administrativa; las personas con discapacidad sensorial en situación de dependencia reconocida por resolución administrativa; las personas que padezcan una enfermedad mental diagnosticada en situación de dependencia reconocida por resolución administrativa, y las personas que estando en situación de riesgo de aislamiento social, se les detecte por el servicio social de base necesidades que pueden ser atendidas por el servicio de teleasistencia, siendo necesario en estos casos la emisión por el servicio social de base del correspondiente informe[103]. A su vez, la teleasistencia se divide en tres grupos: la teleasistencia domiciliaria, la teleasistencia móvil y la telelocalización.

El término de la teleasistencia domiciliaria fue empleado inicialmente en la década de los 90 como un sistema de atención en el domicilio de las personas necesitadas de ayuda en una situación de urgencia, dado que debía de ser un servicio de fácil acceso, se basaba fundamentalmente en el teléfono[104]. Por su parte, la fundación Alzheimer lo ha definido como un servicio preventivo, inmediato y permanente, para la atención de las personas mayores, discapacitadas o con elevado nivel de dependencia, que satisface y moviliza los recursos tecnológicos y sociales necesarios para resolver cualquier situación de necesidad o emergencia y que tiene por objetivo mejorar la calidad de vida de los usuarios facilitando el contacto con su entorno social y familiar y asegurando la intervención inmediata en crisis personales, sociales o médicas para proporcionar seguridad y contribuir decisivamente a evitar ingresos innecesarios en centros residenciales[105].

El dispositivo se organiza en torno al usuario y es sensible a cualquier eventualidad que ocurra en su hogar. A través de una serie de dispositivos telemáticos, ofrece una central de alarmas disponible durante las 24 horas del día, convirtiéndose de esta manera, en una herramienta que otorga seguridad tanto a los usuarios, sobre todo para aquellos que pasan la mayor parte del tiempo solos, como a sus familiares, dado que puede intervenir

[102] Artículo 1 del Decreto 144/2011
[103] Artículo 9 del Decreto 144/2011
[104] MATÍNEZ RAMOS, C., "Las TIC en la Hospitalización y en la Atención Domiciliarias", *Reduca*, Vol. 1, Núm. 1, 2009, p. 280
[105] FUNDACIÓN ALZHEIMER ESPAÑA., "Teleasistencia: ¿Qué es? ¿En qué consiste? ¿Cómo contratarlo?", *alzfae*, disponible en: http://www.alzfae.org/fundacion/459/teleasistencia-que-es-en-que-consiste-como-contratarlo *[Última consulta: 27 de mayo de 2021]*

instantáneamente y de forma personalizada sobre sus necesidades específicas sin necesidad de institucionalizarlos[106]. Sus funciones son las siguientes: favorecer la permanencia y la integración de las personas en el medio habitual en que desarrollan su vida, evitando con ello situaciones de desarraigo y el ingreso innecesario, y no deseado, en instituciones; potenciar y mantener el mayor grado de autonomía e independencia de las personas en su domicilio durante el mayor tiempo posible, favorecer la seguridad y la confianza de las personas mayores, proporcionando una intervención y una atención rápida en caso de crisis personales, sociales o sanitarias, y proporcionar tranquilidad para el usuario[107].

A la forma de teleasistencia domiciliaria se la conoce fundamentalmente con el término de "Telealarma", servicio que se estructura sobre dos unidades: la unidad central y la unidad domiciliaria. La primera está formada por los dispositivos requeridos y los profesionales técnicos formados para atender las llamadas desde el centro de atención. La segunda, es la que se constituye en el domicilio del usuario y consta de dos terminales: terminal fijo, compuesto de altavoz y micrófono que se suele colocar junto al teléfono del usuario, y el terminal inalámbrico, que el usuario se pone a modo de colgante[108].

En cuanto a su funcionamiento, a través de un medallón colgado en el cuello de la persona, una terminal de teleasistencia y una línea telefónica, el usuario está conectado continuamente con un operador de centro de control. El usuario simplemente ha de apretar el botón rojo para pedir ayuda, transporte sanitario, o simplemente para charlar. El teleoperador que disponga de una base de datos con todos los datos médicos y personales atenderá a la llamada y pondrá en marcha los recursos adecuados para ayudar al usuario de la forma más rápida posible (movilizando parientes, vecinos, ambulancias, médicos, bomberos, policía local, voluntarios, asistentes sociales, etc.). Si un usuario hace sonar la alarma, inmediatamente aparecerá una ventana en el ordenador de todos los operadores con los siguientes datos: un número de teléfono, un código de usuario y el tipo de pulsación, colgante o terminal.

El operador que responda a la llamada solo tendrá que hacer doble-click sobre la ventana, y la llamada desaparecerá de la bandeja de entrada, simultáneamente, en una unidad de almacenamiento de audio digital, se grabará la llamada mientras se realiza la intervención. Frente al operador, en su pantalla, se desplegará una interfaz dinámica con los datos del usuario que solicita ayuda: datos personales, diagnósticos clínicos, medicamentos, profesionales sanitarios que lo atienden, personas allegadas con llaves del domicilio y sin llaves, notas dejadas por otros operadores sobre el usuario, etc.

[106] TIRADO, F.; LÓPEZ, D., CALLÉN, B. y DOMÈNECH, M., "La producción de fiabilidad en entornos altamente tecnificados. Apuntes etnográficos sobre un servicio de teleasistencia domiciliaria", *Papeles del CEIC*, Vol. 2, Núm. 38, 2008, p. 14

[107] GIL GONZÁLEZ, S. y RODRÍGUEZ-PORRERO, C., Tecnología y personas mayores, *Instituto de Mayores y Servicios Sociales*, 2017, pp. 52-53, disponible en: https://www.imserso.es/InterPresent1/groups/imserso/documents/binario/122017001_tecnologia-y-persona.pdf

[108] GONZÁLEZ RAMÍREZ, A. y MORA LIMA, V., *Teleasistencia*, McGraw-Hill, Madrid, 2013, p. 11

Gracias a todo esto, el operador esbozará un personaje y una conjetura sobre lo qué está ocurriendo. Una vez que se sepa lo que está ocurriendo, deberá intervenir para solventar las necesidades de sus usuarios, y esto comprende realizar tareas administrativas, conversar con el usuario y/o movilizar algún recurso de urgencia[109].

Respecto a la teleasistencia móvil, esta modalidad de teleasistencia permite una atención del usuario fuera del domicilio similar a la de la teleasistencia básica. Tiene los mismos objetivos que la teleasistencia doméstica, sumando uno más: facilitar la salida de su domicilio a las personas mayores, incrementando de esta forma su movilidad y seguridad. El servicio consta de un centro de atención, unidad operativa especializada desde donde se gestiona la atención a los usuarios teleasistidos; una plataforma tecnológica, que se traduce como infraestructura de servidores, comunicaciones de la plataforma de teleasistencia y software; y un terminal móvil de teleatención de fácil utilización y con un número reducido de teclas que permite canalizar las alertas emitidas por el usuario y por los sensores con los que cuenta, así como una comunicación telefónica con el centro de atención[110]. Las funcionalidades que presta la plataforma y el centro de atención son similares a las de la teleasistencia básica. Pero, en caso de emergencia, y si el terminal cuenta con localización GPS, es posible localizar geográficamente al usuario en situación de riesgo.

Por último, la telelocalización es un servicio de teleasistencia para usuarios que tienen la suficiente autonomía como para pasear o moverse en un espacio determinado de su entorno, pero padecen un deterioro cognitivo. Se trata de personas con alzhéimer u otras demencias que, al encontrarse en sus fases iniciales, todavía pueden moverse con cierta autonomía en su propio entorno, pero controlando las situaciones de riesgo en las que puedan incurrir. A diferencia de la teleasistencia móvil, el usuario no realiza una interacción, siendo el personal del centro de atención el que debe estar atento a las alertas que automáticamente genere el terminal del usuario y seguir el protocolo previsto para cada incidencia. Son servicios distintos tanto desde el punto de vista de la tipología de los usuarios, de los protocolos de actuación y de la configuración de la plataforma y de los terminales, aunque pueden compartir la misma tecnología. El mayor problema es que, cuando se utiliza el GPS, el servicio se mueve en una situación de difícil equilibrio entre las necesidades de seguridad del usuario y su derecho a la protección de datos personales[111].

b) Riesgos que plantea la teleasistencia desde la perspectiva del derecho a la protección de datos personales:

Para poder proporcionar una atención sanitaria de calidad y una rápida respuesta en situaciones de emergencia, la unidad central ha de contar con una ficha de cada usuario

[109] TIRADO, F.; LÓPEZ, D.; CALLÉN, B. y DOMÈNECH, M., "La producción de fiabilidad en entornos altamente tecnificados. Apuntes etnográficos sobre un servicio de teleasistencia domiciliaria", *cit.*, pp. 14-17
[110] GIL GONZÁLEZ, S. y RODRÍGUEZ-PORRERO, C., Tecnología y personas mayores, *cit.*, pp. 59-61
[111] Ibid., pp. 59-63

donde se recoja detalladamente la información sanitaria de cada uno. Aunque sea necesario que en la unidad central cuenten con todos estos datos, este mismo hecho crea riesgos desde la perspectiva del derecho a la protección de datos personales del usuario mayor, puede haber una venta de datos, vicios en el consentimiento o accesos no autorizados entre otras cuestiones.

En el año 2018 la sección sindical de la Confederación General del Trabajo comenzó un proceso contra el Servicio Andaluz de Teleasistencia[112] ante la Agencia Española de Protección de Datos por introducir una cláusula demasiado genérica en el documento denominado "estatutos del servicio" que no especificaba ni el tipo de datos a almacenar, ni el uso o cesiones previstos. Una vez registrada la solicitud, las personas usuarias firmaban un documento de adhesión al Servicio de Teleasistencia, indicando que habían recibido información sobre el servicio y habían leído y aceptado en todos sus términos las condiciones generales, pero para prestar correctamente el servicio, en el momento de la instalación de los dispositivos por parte del adjudicatario, (la entidad PROAZIMUT) se recaba un cuestionario con diversos datos sin que se proporcionara información se sobre la recogida, tratamiento o finalidad de los datos. Esto es, se producía una primera recogida de datos en el impreso de petición del servicio, pero, posteriormente, en el momento de la instalación de los dispositivos en los domicilios, se realizaba una recogida de datos más amplia.

Con la firma de la solicitud del servicio y la información que en el mismo se contenía se cumplía con el deber de informar al usuario. Sin embargo, no solo se recogían datos en ese impreso de solicitud, sino que se realizaba una recogida más extensa y detallada de datos de salud en el momento posterior de instalación de los dispositivos en los domicilios de los afectados. El impreso de solicitud originario no informaba sobre dicha nueva recogida, incumpliendo con el deber de informar del responsable del tratamiento, ya que con carácter previo al correspondiente tratamiento, los interesados debían conocer qué datos eran necesarios para el servicio que se le iba a prestar, y tener un perfecto conocimiento de cuáles eran las finalidades para las que se tratarían los datos y, en su caso, para qué y a quien eran cedidos, puesto que solo así podrían ejercer el poder de disposición y control sobre sus datos personales.

Por todo ello, la AEPD en su resolución de 28 de mayo de 2019, resolvió que se debía reforzar el contenido de la cláusula informativa de la solicitud del servicio en la que exclusivamente se indicaba la incorporación de los datos a un fichero y la sede de ejercicio de los derechos, así como en el documento de adhesión, o unificar la

[112] El SAT es una prestación de la Junta de Andalucía de atención personalizada que permite a sus usuarios mantener contacto verbal a través de línea telefónica disponible las 24 horas del día todos los días siendo su fin, entre otros, conseguir y mantener el grado de autonomía e independencia de las personas mayores en su domicilio, proporcionar a las personas mayores seguridad y una atención rápida en casos de emergencia y atención directa con seguimiento personal de cada usuario. La persona que solicite el servicio de teleasistencia domiciliaria, rellena un impreso de solicitud en el que entre otras cuestiones se recogen datos de carácter personal como la edad, enfermedad o el grado de discapacidad, a cumplimentar a mano, este impreso lleva la firma del titular peticionario o representante legal.

información en el primer documento haciendo una referencia más extensa de los datos a recoger en cuanto a su finalidad y contemplando exclusivamente los datos necesarios[113].

En cuanto a la teleasistencia móvil, es una modalidad de teleasistencia que permite una atención del usuario fuera del domicilio similar a la de la teleasistencia básica, pero ante situaciones de riesgo puede activarse la geolocalización para localizar al usuario. La cuestión es que, tal y como se ha indicado anteriormente, cuando se utiliza la geolocalización los servicios se mueven en una situación de difícil equilibrio entre las necesidades de seguridad del usuario y su derecho a la protección de datos. Esta situación tan delicada puede apreciarse claramente en el caso de la telelocalización, en el cual es posible que las personas usuarias del servicio no sean conscientes de la supervisión de la que son objeto, es posible que los usuarios no sean realmente conscientes de que su localización está siendo controlada constantemente. Por ello, es indispensable que en el contrato se especifique claramente cómo se realizara dicho control, y que el usuario acepte libremente utilizar este sistema.

3.2.3. Telemonitorización:

a) Concepto:

Se define como el uso de las TIC para monitorear a distancia a los pacientes[114]. El monitoreo puede realizarse de forma continua o puntual. En el caso de forma continua, el usuario lleva continuamente un dispositivo que realiza las medidas y almacena los datos, y estos datos se envían al médico, siendo posible programar alarmas en caso de que determinados valores excedan los límites aconsejables, el médico también puede consultar remotamente los datos en cualquier momento. En el caso de la forma puntual, es necesaria la colaboración del paciente para que el médico pueda medir los parámetros remotamente. Es el caso, por ejemplo, del empleo de glucómetros o espirómetros, que miden los niveles de glucosa o capacidad respiratoria respectivamente[115].

Este sistema potencia la capacidad del paciente para la autogestión del cuidado, manejo y control de su propia enfermedad, mejora el cumplimiento terapéutico, facilita la detección y actuación precoz en las descompensaciones o exacerbaciones de sus patologías y facilita la recuperación en el domicilio tras episodios que requieran ingresos hospitalarios. Además, el empleo de estas tecnologías aplicadas en el cuidado domiciliario puede mejorar la calidad de vida de los pacientes[116]. Como bien se ha

[113] Resolución de la AEPD R/00103/2019 de 28 de mayo de 2019 (Procedimiento nº AP/00060/2018)
[114] MEYSTRE, S., "The current state of telemonitoring: a comment on the literature", *Telemedicine Journal & e-Health*, Vol. 11, Núm. 1, 2005, p. 63
[115] GARCÍA MARTÍNEZ, N. y BERMEJO NIETO, A., "Tecnologías de la información y las comunicaciones para las personas mayores", *Universidad Politécnica de Madrid*, 2004, p. 48, disponible en: https://www.upm.es/sfs/Rectorado/Organos%20de%20Gobierno/Consejo%20Social/Actividades/tecnologias_informacion_comunicaciones.pdf
[116] MARTÍN-LESENDE, I.; ORRUÑO, E.; BAYÓN, J.C.; BILBAO, A.; VERGARA, I.; CAIRO, M.C.; ASUA, J.; ROMO, M.I.; ABAD, R., REVIRIEGO, E. y LARRAÑAGA, J., "Evaluación e impacto de una intervención de telemonitorización en pacientes domiciliarios con insuficiencia cardiaca o

indicado anteriormente, al igual que la teleasistencia, la telemonitorización o monitorización remota, es una especialidad dentro de la telemedicina que cobra especial importancia en el caso de las personas mayores.

Entre los dispositivos que se utilizan en la telemonitorización pueden citarse los glucómetros de sangre, oxímetros de pulso, básculas, marcapasos cardíacos, etc. Estos dispositivos se conectan al paciente para recolectar todo tipo de datos relacionados con su salud, y algunos tienen la posibilidad de generar alertas cuando se exceden los límites preestablecidos por el personal sanitario. Una vez se hayan recolectado los datos de los pacientes, se transfieren mediante diferentes vías como Bluetooth o Wi-Fi a las historias clínicas electrónicas o aplicaciones móviles[117]. Es decir, los datos "viajan" a través de múltiples dispositivos y redes de comunicación, para posteriormente ser analizador por una máquina y/o profesional.

En el País Vasco se realizó un ensayo clínico llamado TELBIL[118] para evaluar el impacto de una intervención de telemonitorización en pacientes domiciliarios con capacidad respiratoria y/o broncopatía crónica en comparación con la práctica clínica habitual, siguiendo a los pacientes durante un año. El seguimiento basado en la telemonitorización, consistió en el envío diario desde el domicilio de los siguientes parámetros clínicos del paciente de forma no automatizada: frecuencia respiratoria, frecuencia cardiaca, tensión arterial, saturación de oxígeno en sangre medida mediante pulsioximetría, peso y temperatura; además de un breve cuestionario que recogía la percepción de su situación clínica y funcional respecto al día anterior, e ítems de recuerdo del seguimiento de medicación y dieta que se enviaron junto con los parámetros clínicos. Los profesionales sanitarios (médico o enfermera de referencia habitual en su centro de salud), revisaron diariamente los datos, y el personal de enfermería mantuvo contacto telefónico quincenal rutinario con el paciente. Asimismo, siempre que se consideró necesario, y como consecuencia de variaciones clínicas de los datos recibidos en los Centros de Atención Primaria, se contactó telefónicamente con el paciente. El sistema de telemonitorización se completó implantando unas alertas individualizadas para cada paciente, que avisaron en la plataforma Web cuando los parámetros introducidos quedaron fuera de los rangos establecidos, lo que facilitó la revisión de datos. Se establecieron una serie de combinaciones de alertas para que desde la propia terminal del Asistente Digital Personal *"Personal Digital Assistant"* (PDA), conocidos como ordenadores de mano (por ejemplo, los teléfonos inteligentes o las tablets), se sugiriese a los pacientes contactar con un servicio de urgencias durante los

---

broncopatía crónica controlada desde la atención primaria. Ensayo clínico aleatorizado. Estudio TELBIL", *Servicio Central de Publicaciones del Gobierno Vasco*, 2013, p. 25, disponible en: https://www.osakidetza.euskadi.eus/contenidos/informacion/2013_osteba_publicacion/es_def/adjuntos/INTERVENCION%20DE%20TELEMONITORIZACION.pdf

[117] BHATTACHARYYA, S.B., *A DIY Guide to Telemedicine for Clinicians*, Springer, Singapur, 2017, pp. 59 y 72

[118] MARTÍN-LESENDE, I.; ORRUÑO, E.; BAYÓN, J.C.; BILBAO, A.; VERGARA, I.; CAIRO, M.C.; ASUA, J.; ROMO, M.I.; ABAD, R., REVIRIEGO, E. y LARRAÑAGA, J., "Evaluación e impacto de una intervención de telemonitorización en pacientes domiciliarios con insuficiencia cardiaca o broncopatía crónica controlada desde la atención primaria. Ensayo clínico aleatorizado. Estudio TELBIL", *cit.*, pp. 34 y 83

fines de semana, fuera del horario de cobertura del Centro de Salud. Al resto de los pacientes, se les realizó el seguimiento mediante los cuidados habituales además de la telemonitorización.

Este estudio indicó que la telemonitorización controlada directamente desde la Atención Primaria incrementa el porcentaje de pacientes domiciliarios sin ningún ingreso hospitalario tras un año de seguimiento con respecto a los pacientes a los que se les aplica el seguimiento mediante la práctica habitual. Se apreció una tendencia tanto a sufrir un menor número de ingresos hospitalarios por cualquier causa y específicos, como a una disminución de la estancia hospitalaria entre los pacientes telemonitorizados. Finalmente, se entendió fundamental considerar la repercusión de la intervención de telemonitorización en la reorganización asistencial, en los profesionales sanitarios y en los pacientes-familiares[119].

b) Riesgos que plantea la telemonitorización desde la perspectiva del derecho a la protección de datos personales:

Los sistemas de monitorización remota de pacientes deben garantizar tanto la privacidad de los mismos como la calidad de la información de los datos recolectados. Una vez se hayan recogido los datos, estos "viajan" a través de múltiples dispositivos y redes de comunicación, para posteriormente ser analizados por una máquina y/o profesional, quedando expuestos a ciberataques. De la misma manera, los propios dispositivos necesitan utilizar una variedad de mecanismos de conectividad para funcionar correctamente, quedando expuestos a los defectos de diseño[120].

Actualmente, existen diversos proyectos de telemonitorización tanto a nivel nacional como europeo dirigidos a personas mayores, cuyo fin es monitorizar la salud de los participantes mediante dispositivos llevables y sensores colocados en sus hogares que permiten a los profesionales sanitarios mejorar la toma de decisiones sanitarias personalizadas. Uno de los principales problemas que plantean este tipo de proyectos lo constituye el consentimiento del interesado que, tal y como se expondrá detalladamente más adelante, es una de las bases legitimadoras para el tratamiento de los datos relativos a la salud. La hoja informativa ha de estar redactada teniendo en cuenta las características de los participantes, para cumplir adecuadamente con el deber de informar del responsable del tratamiento. De la misma manera, el documento del consentimiento del interesado ha de estar compuesto de frases sencillas y comprensibles para las personas mayores que no están habituadas a las nuevas tecnologías para que el tratamiento pueda considerarse lícito.

---

[119] Véase igualmente un estudio realizado por la Generalitat Valenciana: GENERALITAT VALENCIANA., "Telemonitorización en pacientes con patologías crónicas en Atención Primaria. Programa Valcrònic", 2016, pp. 27-29, disponible en: http://publicaciones.san.gva.es/publicaciones/documentos/V.1481-2016.pdf

[120] BHATTACHARYYA, S.B., A DIY Guide to Telemedicine for Clinicians", *cit.*, pp. 48-49

3.3. Un desarrollo reciente, la salud móvil:

3.3.1. Concepto:

Este término fue creado para identificar las tecnologías de redes y comunicaciones móviles para el cuidado de la salud[121]. Según la OMS[122], la salud móvil ("*mobile health*" o "*Mhealth*") es la práctica de la medicina y la salud soportada por dispositivos móviles como teléfonos, dispositivos de monitorización de pacientes, asistentes digitales y otros dispositivos inalámbricos. Los dispositivos móviles son parte de las TIC, por lo que la salud móvil es un subconjunto de la salud digital, que hace referencia al uso de dispositivos móviles para el cuidado de la salud. El término incide en el aspecto de movilidad que permiten estas herramientas, lo cual posibilita que los pacientes estén conectados en cualquier momento y lugar.

Existen numerosos dispositivos que se utilizan para recabar datos del usuario, y una vez recolectados, son volcados a una aplicación informática mediante distintos sistemas. Estas aplicaciones informáticas pueden estar instaladas en el teléfono o Tablet del usuario. En otras situaciones, como puede ser el caso del teléfono, es el mismo dispositivo el que recolecta los datos, no habiendo volcado de datos, dado que en este caso la aplicación informática que analizará los datos se encuentra en el mismo dispositivo. En suma, los dispositivos y las aplicaciones van de la mano.

Esta subcategoría de la salud digital engloba desde la prevención y el diagnóstico clínico hasta el tratamiento de pacientes, convirtiéndose en un instrumento clave en la comunicación entre diversos profesionales de la salud, así como entre facultativos y pacientes. La salud móvil permite la recogida de un considerable número de datos médicos, fisiológicos y relativos al modo de vida, a la actividad diaria y al entorno de la persona plateada, pudiendo servir de base para el ejercicio de una práctica sanitaria y actividades de investigación basadas en resultados comprobados, al tiempo que facilita el acceso de los pacientes a su información sanitaria en cualquier lugar y en cualquier momento[123].

Una de las principales características de la salud móvil es el flujo de información continuo entre el usuario o paciente y el profesional sanitario, permitiendo diagnósticos precoces o la monitorización de pacientes crónicos, dependientes o de riesgo. Asimismo, posibilita que la atención sanitaria llegue a zonas rurales, evitando en la mayoría de los casos, que los pacientes tengan que trasladarse hasta los centros sanitarios, puesto que, gracias a las herramientas de la salud móvil, los profesionales sanitarios pueden asesorar y seguir a sus pacientes mediante un servicio remoto.

---

[121] ISTEPANIAN, R.; LAXMINARAYAN, S.; PATTICHIS, C., *M-health: Emerging mobile health systems*, Springer, Nueva York, 2007, p. 3

[122] OMS., "mHealth: New horizons for health through mobile technologies", *OMS*, 2011, p. 6, disponible en: http://apps.who.int/iris/bitstream/handle/10665/44607/9789241564250_eng.pdf?sequence=1

[123] COMISIÓN EUROPEA. Libro verde sobre sanidad móvil, 2 de mayo de 2014, p. 3

Se ha dicho que la salud móvil otorga poder al usuario plateado, el médico no debe entenderse como el único "guardián" de la salud, el paciente mayor debe ser consciente de que tiene que asumir un rol activo y comenzar a preocuparse por su salud adquiriendo unos hábitos de autovigilancia y control. Estas tecnologías dotan a las personas mayores de unas herramientas de control, cuidado y prevención que les permitan participar activamente en el proceso[124]. Las soluciones de sanidad móvil refuerzan el cambio de un papel pasivo a un papel más participativo de los pacientes, al tiempo que se refuerza la responsabilidad sobre su propia salud mediante sensores que detectan e informan de las constantes vitales y aplicaciones móviles que les ayudan a cumplir con la dieta y la medicación. Contribuye a la capacitación de los pacientes mayores, ya que estos pueden llegar a gestionar su salud de manera más activa, con vidas más independientes en el entorno de sus propios hogares, gracias a la autoevaluación o a soluciones de seguimiento a distancia. El objetivo no es sustituir a los profesionales sanitarios, que siguen siendo esenciales para proporcionar atención sanitaria, sino fomentar el apoyo para la gestión y la prestación de la atención sanitaria[125].

3.3.2. Riesgos que plantea la salud móvil desde la perspectiva del derecho a la protección de datos personales:

En la medida en que la salud móvil es una modalidad de Internet de las cosas, los riesgos que plantea la salud móvil desde la perspectiva del derecho a la protección de datos son, entre otros, el perfilado y la discriminación, la anonimización o los ciberataques. A estos riesgos nos hemos referido anteriormente.

Respecto a las aplicaciones móviles que se utilizan en la salud móvil, tal y como se ha dicho en su respectivo apartado, estos plantean numerosos riesgos desde la perspectiva de la protección de datos, y más aún cuando el usuario es una persona mayor. Recordemos que los principales riesgos para la protección de los datos de los usuarios mayores son la falta de transparencia y conocimiento de los tipos de tratamiento que las aplicaciones pueden realizar, el consentimiento, la clara tendencia hacia la maximización de los datos, las insuficientes medidas de seguridad y el grado de fragmentación de los numerosos actores que intervienen en el desarrollo de aplicaciones.

Las aplicaciones, han de estar acreditadas por un organismo que garantice su calidad y seguridad. Si no se ha realizado dicha acreditación, el usuario se encuentra ante potenciales amenazas de seguridad, y en el caso de las aplicaciones médicas, pueden crearse riesgos para la salud del paciente. Es necesario que los usuarios cuenten con fuentes transparentes de información sobre su calidad, para decidir cuál es la aplicación más apropiada para sus necesidades.

[124] NIÑO GONZÁLEZ, J.I. y FERNÁNDEZ MORALES, B., "Comunicación, Salud y tecnología: mHealth", Revista de comunicación y salud, Vol. 5, 2015, p. 149
[125] COMISIÓN EUROPEA. Libro verde sobre sanidad móvil, *cit.*, pp. 3-6

Algunas veces, los datos se almacenan en el mismo dispositivo del usuario, sin embargo, en otras situaciones, se almacenan en la nube. En estos casos, entran el juego los referidos riesgos que crea el Cloud Compunting desde la perspectiva del derecho a la protección de datos, como la falta de transferencia sobre donde se encuentran realmente los datos, con todo lo que ello conlleva, o los accesos a los datos relativos a la salud de los hackers. Los numerosos actores que intervienen en el desarrollo de aplicaciones también suponen un riesgo grave para la protección de datos. Para alcanzar el máximo nivel de privacidad y protección de datos, deben colaborar todas las partes del ecosistema de las aplicaciones. Es necesario determinar cuáles son las medidas de seguridad que se han de implementar por cada uno de los distintos intervinientes y que la normativa recoja la responsabilidad que tendrán los participantes en cada momento.

En suma puede decirse que la sanidad móvil tiene el potencial de desempeñar un papel importante para mejorar la vida de las personas mayores. Sin embargo, resulta indispensable garantizar que estos puedan utilizar la tecnología con total seguridad, respetando en todo momento su derecho a la protección de datos. La alfabetización digital cobra especial importancia en este campo, puesto que, gracias al conocimiento informático adquirido, las personas mayores comprenderán lo que suponen y podrán decidir libremente si quieren utilizarlas o no.

CAPÍTULO 2: LA NUEVA REALIDAD JURÍDICA DE LAS PERSONAS MAYORES CON DISCAPACIDAD TRAS LA ENTRADA EN VIGOR DE LA LEY 8/2021 POR LA QUE SE REFORMA LA LEGISLACIÓN CIVIL Y PROCESAL PARA EL APOYO A LAS PERSONAS CON DISCAPACIDAD EN EL EJERCICIO DE SU CAPACIDAD JURÍDICA

1. INTRODUCCIÓN:

El ordenamiento civil tradicional dictaba que, las personas con discapacidad debían ser privadas de su capacidad de obrar padeciendo una suerte muerte civil y de sustitución que se entendía en beneficio del incapacitado. Esta concepción paternalista de los derechos de la persona con discapacidad, se agravaba en el caso de las personas mayores con discapacidad, por considerarlas personas altamente vulnerables. La sustitución de la voluntad de estas personas por medio de instituciones representativas como la tutela[126] era una práctica habitual y muy extendida, incluso en los casos en los que la persona mayor se podía valer por sí misma en muchos ámbitos de su existencia.

Como es sabido, la reforma operada por la Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica, pretende adaptar la normativa a la Convención de Nueva York de 2006 para que las personas con discapacidad puedan tomar sus propias decisiones mediante el apoyo que necesiten. El objetivo es cambiar el sistema anterior basado en la sustitución de la voluntad por el de apoyos, con el fin de que las personas con discapacidad recuperen el control de sus vidas. La persona encargada de asistir o apoyar a la persona con discapacidad se configura como un ayudante que le asiste en la toma de decisiones, fomentando su libertad y autonomía.

El objetivo de este capítulo consiste en observar adecuadamente los aspectos más importantes de la nueva norma que afectan al ejercicio de la capacidad de las personas mayores con discapacidad. Previamente, para comprender el cambio que se ha producido en el ordenamiento jurídico tras su entrada en vigor expondremos los aspectos más salientes de la reforma operada por la Ley 8/2021. De esta forma estaremos en condiciones de calibrar adecuadamente el cambio de paradigma que supone la citada norma para la vida civil de las personas mayores con discapacidad, siendo necesario realizar una nueva interpretación de la normativa de protección de datos para adecuar la misma a la actual realidad jurídica. Es cierto que existen multitud de trabajos sobre esta reforma y sus antecedentes, pero creemos que es imprescindible recordar dicha evolución, debido a que la misma, y más concretamente el artículo 12 de la Convención de Nueva York, son la base, la razón de ser de la nueva Ley. Una vez realizado este repaso, se identificarán los principales cambios que ha producido la reforma, para pasar a continuación, a describir las medidas de apoyo tanto voluntarias, judiciales como informales que asistirán a las personas mayores con discapacidad.

[126] Véase al respecto: GIL RODRÍGUEZ, J., "La tutela como garantía de las personas incapacitadas y del respeto de sus derechos", *Revista del poder judicial*, Núm. 81, 2006

Entender el sentido y alcance de cada medida permitirá saber cómo podrán ser utilizadas en el ámbito de la protección de datos personales, lo cual será analizado en los siguientes capítulos. Por ello, este capítulo se constituye como instrumento necesario para comprender, entre otras cuestiones, el efecto que el nuevo sistema de apoyos produce en la capacidad de las personas mayores con discapacidad a la hora de otorgar el consentimiento para el tratamiento de sus datos relativos a la salud, lo cual será analizado en los siguientes capítulos.

2. CONTEXTO SOCIOLÓGICO EN EL QUE SE PRODUCE LA REFORMA DE LA DISCAPACIDAD:

Antes de comenzar a analizar el cambio que ha conllevado la entrada en vigor de la Ley 8/2021, es necesario analizar los distintos términos que desde la realidad sociológica han servido para identificar al colectivo que nos ocupa. El objetivo de este ejercicio es comprender con mayor detalle la evolución que han sufrido los términos, y qué efecto han tenido estas etiquetas o conceptos jurídicos en la vida civil de las personas mayores con discapacidad, lo cual nos permitirá entender de una forma más adecuada el núcleo de esta reforma.

2.1. La vejez o ancianidad y la tercera y cuarta edad:

Según la Real Academia Española de la lengua (RAE), la vejez es la cualidad de viejo. Es un concepto cambiante, puesto que, al tiempo que se incrementa el número de personas mayores, el umbral de la vejez tiende a alejarse[127]. Llama la atención la segunda definición que se ofrece sobre el concepto de la vejez: "edad senil, senectud". Esto es, se equipara la vejez con los problemas de demencia; afirmación criticable ya que múltiples autores han denunciado el estigma con el que la RAE define el fenómeno de la vejez, a la que se asocia una connotación peyorativa[128]. La ancianidad es otro término equivalente que también se usa para referirse al colectivo de las personas mayores, definiéndose como "el último periodo de la vida del ser humano"[129].

En la década de 1970 se realizó una distinción entre "viejos-jóvenes" ("*young old*") y "viejos-viejos" ("*old-old*"), refiriéndose a la tercera y cuarta edad respectivamente. Según este enfoque, la tercera edad se caracterizaría todavía como una fase de la vida en la que las personas son aun autónomas e independientes; en cambio, la cuarta edad se

[127] MINGORANCE GOSÁLVEZ, C., "Delimitación del término persona mayor en la ley andaluza de atención y protección a las personas mayores", en PÉREZ VARGAS MUNOZ, J. y PEREÑA VICENTE, M., *La encrucijada de la incapacitación y la discapacidad*, Wolters Kluwer, Madrid, 2011, p. 482

[128] Bajo el lema de "eliminemos las aceptaciones despectivas en la definición de vejez", se creó un movimiento para la recaudación de firmas contra la definición emanada por la RAE. UNATE., "Eliminemos las acepciones despectivas en la definición de vejez", *change.org*, disponible en: https://www.change.org/p/real-academia-espa%C3%B1ola-cambio-en-la-definici%C3%B3n-de-la-palabra-vejez-en-la-rae *[Última consulta: 17 de mayo de 2022]*

[129] RAE., Definición de ancianidad, disponible en: https://dle.rae.es/ancianidad *[Última consulta: 17 de mayo de 2022]*

entiende como un deterioro que lleva a la enfermedad y a la dependencia[130]. Entre fines de la década de 1980 y principios de 1990, se vinculó la cuarta edad con altos índices de morbilidad, no obstante, una serie de estudios longitudinales mostraron que no todas las personas que superan los 80 años son dependientes y que esta condición ha mejorado con la incorporación de las nuevas tecnologías [131].

La dificultad de precisar jurídicamente quiénes son las personas mayores se solventa estableciendo franjas de edad. En este sentido, algunas leyes autonómicas conceden prestaciones sociales a las personas mayores de sesenta y cinco años, sin que pueda decirse que todos compartan idénticas circunstancias sociales, económicas, físicas o familiares[132]. En la Exposición de Motivos de la Ley 6/1999, de 7 de julio, de Atención y Protección a las personas Mayores de la Comunidad Autónoma de Andalucía[133], se habla de la "realidad cambiante y diversa que las personas presentan a partir de los sesenta y cinco años". La citada ley establece la edad de sesenta y cinco años como circunstancia a partir de la cual puede considerarse que una persona es "mayor". Criterio que a su vez es discutible, puesto que, según ZURITA MARTÍN, la persona mayor y el jubilado son dos términos que en ningún caso deben entenderse como sinónimos o términos equiparables[134].

En el presente trabajo, se ha optado por emplear los términos "persona mayor" o "personas de edad avanzada" evitando otros como "personas de la cuarta edad" o "ancianos", al considerar que los mismos son términos respetuosos para referirse a este sector poblacional y suficientemente generales como para comprender todas las facetas abarcables de dicho periodo.

2.2. El edadismo:

Hemos dicho que la vejez posee tintes o connotaciones negativas en las sociedades contemporáneas. En cambio, es interesante constatar que no siempre ha sido así. En las sociedades primitivas se valoraba la edad, las personas mayores a menudo proporcionaban conocimiento, experiencia y memoria institucional; conocimiento y experiencia que era de valor, incluso en términos de mayor posibilidad de supervivencia, para sus sociedades. Sin embargo, en distintos períodos de la historia de la cultura y de las civilizaciones, han surgido opiniones, evaluaciones y juicios opuestos sobre la vejez. La edad avanzada ha sido valorada tanto de forma positiva como negativa. La primera visión hace referencia a la consideración de la persona mayor

[130] Se define la cuarta edad como periodo de edad sucesorio de la tercera edad, iniciado a los 80 años, determinado por un descenso de capacidades físicas, mentales y orgánicas, precedido por la cronicidad, la disfunción y la dependencia. Véase al respecto: MORENO TOLEDO, A., "La cuarta edad. Perfil conceptual de la vejez avanzada", *Poiésis*, Vol. 10, Núm. 20, 2010, p. 4.

[131] ODDONE, M.J. y POCHINTESTA, P., "La cuarta edad: la fragilidad en cuestión", en PAREDES, M. y MONTEIRO, L. (coord)., *Desde la niñez a la vejez: nuevos desafios*, Teseo, Buenos Aires, 2019, p. 325

[132] ZURITA MARTÍN, I., *Protección civil de la ancianidad*, Dykinson, Madrid, 2004, p. 16

[133] BOE núm. 233, de 29 de septiembre de 1999

[134] MINGORANCE GOSÁLVEZ, C., "Delimitación del término persona mayor en la ley andaluza de atención y protección a las personas mayores", *cit.*, pp. 483-485

como sabia, cargada de experiencia, de alto estatus social, merecedora de un gran respeto y con una clara posición de influencia sobre los demás; este punto de vista ha estado arraigado en las sociedades cazadora-recolectoras y agrícolas y ganaderas. La valoración negativa, que es más propia de las sociedades industriales como la neustra, se refiere a la vejez como un estado deficitario, en el cual la persona se encuentra físicamente disminuida, mentalmente debilitada, económicamente dependiente, socialmente aislada y con una disminución del estatus social[135]. Es este último paradigma el que domina las sociedades occidentales avanzadas en las que la vejez es percibida como una situación indeseable y no como una fase vital más, a pesar de que, tal y como afirma GOMÁ LANZÓN[136], vivir es querer envejecer, y querer vivir es querer envejecer.

Con el fin de denunciar la visión peyorativa de la vejez en nuestras sociedades se creó precisamente el concepto del "edadismo*"*. El "edadismo" o "*ageism*" es un término propuesto por BUTLER[137], quien lo definió como "un proceso por el cual se estereotipa y discrimina de forma sistemática a las personas mayores por el simple hecho de ser mayores, de la misma forma que lo hacen el racismo por motivo del color de la piel y el sexismo por el género"[138].

En efecto, es habitual entre nosotros encontrarnos con perjuicios referidos a la fragilidad de los cuerpos de las personas mayores, a la falta de productividad y a su dependencia[139]. La tradición teórica en el campo de la gerontología social atribuye la causa de los problemas en la vejez a la jubilación o la decadencia física[140]. Se trata de una aproximación a la vejez que se focaliza en el análisis del mercado de trabajo y de la jubilación, así como su relación con el empobrecimiento de las personas mayores. Todo ello implica una construcción social de un estatus de dependencia[141]. En la misma línea, el sociólogo LLUIS FLAQUER[142] habla de una situación de semidependencia por parte de los ancianos estructuralmente análoga a la de los parados y de las amas de casa, al encontrarse al margen del proceso de producción económica.

En multitud de ocasiones las personas mayores son tratadas como si fuesen seniles e incompetentes. Basándose en un enfoque paternalista, se les considera como menores desprotegidos a los que hay que proteger. La discriminación de la que son objeto las personas mayores las pone muchas veces en una situación que vulnera sus derechos.

---

[135] CARBAJO VÉLEZ, M.C., "Mitos y estereotipos sobre la vejez. Propuesta de una concepción realista y tolerante", *Ensayos*, Núm. 24, 2009, pp. 88-89

[136] GOMÁ LANZÓN, J., *Ejemplaridad pública*, Taurus, Barcelona, 2015, p. 307

[137] BUTLER, R., *The Encyclopedia of Aging*, Springer, Nueva York, 1987, p. 22

[138] JOHNSON, J. y SLATER, R., *Ageing and later life*, Sage, Londres, 1993, pp. 200-2002

[139] SANDBERG, L., "Affirmative old age- The ageing body and feminist theories on difference", *International Journal of Ageing and Later Life*, Vol.8, Núm.1, 2013, p. 11

[140] En este sentido: MORENO MORENO, J., "Mayores y calidad de vida", *Portularia*, Núm. 4, 2004, 192 y ss

[141] ARLETTAZ, F. y PALACIOS SANABRIA, M.T., *Reflexiones en torno a Derechos Humanos y grupos vulnerables*, Universidad del Rosario, 2015, pp. 131-132

[142] FLAQUER, L., "La emancipación familiar de los jóvenes", *Revista de estudios de juventud*, Núm. 39, 1997, p. 44

2.3. La fragilidad:

Otro de los epítetos normalmente ligados a las características que definen las edades avanzadas es el de fragilidad. Pero, ¿qué significa este término? El diccionario de la RAE afirma que la fragilidad es la "cualidad de frágil"[143]. Frágil, a su vez, significa "quebradizo, y que con facilidad se hace pedazos"[144]. En este sentido, puede decirse que una persona frágil es una persona en situación de riesgo, que puede "romperse" en cualquier momento. Es decir, que puede perder la capacidad para gestionar su vida y por tanto, convertirse en un ser dependiente[145].

Desde un punto de vista clínico se ha definido la fragilidad como un síndrome fisiológico que se caracteriza por la disminución de las reservas y reducción de la resistencia a los estresores como resultado de la declinación acumulativa de múltiples sistemas fisiológicos que incrementan los resultados adversos de salud, entre los que se encuentran: riesgo de enfermedades agudas, caídas y sus consecuencias (lesiones, fracturas), hospitalización, institucionalización, discapacidad, dependencia y muerte[146].

A lo largo de la historia del concepto, se han usado distintos criterios para definir la fragilidad, a saber, criterios médicos (presencia de enfermedades crónicas, alteración de la marcha, déficits sensoriales, caídas reiteradas, polifarmacia, hospitalizaciones frecuentes…), criterios funcionales (dependencia en actividades básicas de la vida diaria), criterios socioeconómicos (vivir solo, viudez, ingresos económicos…), y criterios cognitivos/afectivos (depresión, deterioro cognitivo…)[147]. La pregunta por responder es si el envejecimiento está asociado directamente al concepto de la fragilidad[148].

La palabra "frágil" se asocia a algo delicado o que está por romperse. En este sentido, un adulto mayor frágil es aquel que debido a una disminución de sus reservas fisiológicas, tiene un mayor riesgo de perder su buena salud, lo que lo sitúa en una situación de mayor riesgo de dependencia. Las características de un adulto mayor que empieza el ciclo de la fragilidad desde un punto de vista médico consisten en: pérdida de peso involuntaria, agotamiento, pérdida de fuerza muscular, actividad física reducida y disminución de la velocidad para caminar. Estos cambios se presentan en la mayoría de los adultos mayores, no obstante, la fragilidad requiere algo más ya que no solo se

---

[143] RAE., Definición de fragilidad, disponible en: https://dle.rae.es/fragilidad *[Última consulta: 21 de mayo de 2022]*

[144] RAE., Definición de frágil, disponible en: https://dle.rae.es/fr%C3%A1gil *[Última consulta: 21 de mayo de 2022]*

[145] HURKOA., Informe del proyecto de fragilidad, Vitoria-Gasteiz, 2018, p. 18, disponible en: https://www.hurkoa.eus/sites/default/files/memorias/INFORME_FRAGILIDAD2018_ES_WEB.pdf

[146] ROMERO CARBERA, A.R., "Fragilidad: un síndrome geriátrico emergente", *Medisur*, Vol. 8, Núm. 6, 2010, p.82

[147] JAUREGUI, J.R. y RUBIN, R.K., "Fragilidad en el adulto mayor", *Revista del hospital italiano de Buenos Aires*, Vol. 32, Núm. 3, 2012, pp.110-113

[148] CARRASCO, M., "Fragilidad: Un síndrome geriátrico en evolución", *medicina.uc*, disponible en: https://medicina.uc.cl/publicacion/fragilidad-sindrome-geriatrico-evolucion/ *[Última consulta: 21 de mayo de 2022]*

refiere a la persona sino que depende también de las condiciones en las que vive y de su entorno más próximo[149].

No obstante, debe reconocerse el hecho de que el envejecimiento constituye un proceso de deterioro caracterizado por un aumento de la vulnerabilidad y una disminución progresiva de la reserva fisiológica. Aunque no se traten de sinónimos, la fragilidad se considera altamente prevalente en la vejez; de ahí la necesidad de crear herramientas para promover un envejecimiento activo[150] e independiente.

2.4. La discapacidad:

El tratamiento jurídico de las personas con discapacidad ha ido cambiando al tiempo que la sociedad ha evolucionado. Según la Clasificación Internacional del Funcionamiento, de la discapacidad y de la salud realizada por la Organización Mundial de la Salud (OMS), el concepto de discapacidad englobaba las deficiencias y limitaciones en la actividad, o las restricciones en la participación de las personas[151].

Aunque hace años los conceptos de la minusvalía y discapacidad eran socialmente considerados como sinónimos, la ley ha dispuesto una distinción entre ambas. Así, la Disposición Adicional 8ª de la Ley 39/2006, de 14 de diciembre, de Promoción de la Autonomía Personal y Atención a las personas en situación de dependencia[152], indicó que las referencias que en los textos normativos se efectuaban a "minusválidos" y a "personas con minusvalía", se entenderán realizadas a "personas con discapacidad"; y que, a partir de la entrada en vigor de la citada ley, las disposiciones normativas elaboradas por las Administraciones Públicas utilizarían el término de "persona con discapacidad"[153].

El vocablo minusvalía aplicado a una persona, hace referencia a la disminución del valor de la misma, la devaluación del ser humano. Por ende, se trata de un término con connotación negativa. En cuanto a la discapacidad, se refiere a la situación de la persona

---

[149]RUTE, H., "¿Qué es la fragilidad en los adultos mayores?", *ipsuss*, 16 de mayo de 2018, disponible en:http://www.ipsuss.cl/ipsuss/columnas-de-opinion/que-es-la-fragilidad-en-los-adultos-mayores/2018-05-16/165708.html *[Última consulta: 23 de mayo de 2022]*

[150] El envejecimiento activo es el proceso de optimizar las oportunidades de salud, participación y seguridad a fin de mejorar la calidad de vida a medida que las personas envejecen. Véase al respecto: OMS. Ciudades globales amigables con los mayores: una guía, 2007, p. 10

[151] OMS., "Clasificación Internacional del funcionamiento, de la discapacidad y de la salud", *imserso*, 2001, p. 14, disponible en: https://www.imserso.es/InterPresent2/groups/imserso/documents/binario/435cif.pdf

[152] BOE núm. 299 de 15 de diciembre de 2006

[153] Siguiendo esta línea, el Consejo de Ministros aprobó el Proyecto de reforma del artículo 49 de la Constitución Española, relativo a la protección y promoción de los derechos de las personas con discapacidad en España. Se modifica la terminología que emplea el artículo, eliminando el término de "disminuidos" para referirse ahora al colectivo de las personas con discapacidad. De esta manera, se actualiza el lenguaje de una forma que refleja los propios valores de la Constitución y la dignidad inherente a este colectivo. Véase al respecto: LA MONCLOA., "Reforma del artículo 49 de la Constitución española", *lamoncloa*, 11 de mayo de 2021, disponible en: https://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/110521-enlace-constitucion.aspx *[Última consulta: 24 de mayo de 2022]*

que por sus condiciones físicas o mentales duraderas se enfrenta con notables barreras de acceso a su participación social[154]. Este último término evoca barreras, pero no se refiere a la disminución del valor del sujeto, de ahí que el Comité Español de Representantes de las Personas con Discapacidad (CERMI), lo entienda como el único término válido para referirse al colectivo que nos ocupa[155].

Aunque la Convención Internacional sobre los derechos de las personas con discapacidad de Nueva York de 13 de diciembre de 2006 (en lo sucesivo CDPD o Convención) será analizada más adelante, conviene hacer referencia en este punto a su definición de la discapacidad. La Convención, comienza por indicar en el apartado e) del preámbulo que, la discapacidad es un concepto que evoluciona y que resulta de la interacción entre las personas con deficiencias y las barreras debidas a la actitud y al entorno que evitan su participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás.

Más adelante, el artículo 1.2 del CDPD indica que las personas con discapacidad comprenden a aquellas que tengan deficiencias físicas, mentales, intelectuales o sensoriales a largo plazo que, al interactuar con diversas barreras, puedan ver mermado su derecho a la participación plena y efectiva en la sociedad, en igualdad de condiciones con las demás. Así, según la Convención, las personas con discapacidad son aquellos seres humanos que padeciendo deficiencias (físicas, mentales, intelectuales o sensoriales) de largo plazo, se encuentran con impedimentos y barreras sociales que les impiden o les limitan el ejercicio de sus derechos en igualdad de condiciones.

Por su parte, el Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social[156], señala en su artículo 4.1 que son personas con discapacidad "aquellas que presentan deficiencias físicas, mentales, intelectuales o sensoriales, previsiblemente permanentes que, al interactuar con diversas barreras, puedan impedir su participación plena y efectiva en la sociedad, en igualdad de condiciones con los demás".

Aunque de una primera lectura se pueda entender que se trata de la misma definición que la recogida en el Convenio, lo cierto es que esta última habla de "deficiencias a largo plazo", mientras que la ley se refiere a "deficiencias previsiblemente permanentes". El citado artículo 4.1 de la LGD parte de que las disfunciones se presumen definitivas, por el contrario, la Convención habla de un periodo largo, pero

[154] RAE., Definición de discapacidad, disponible en: https://dle.rae.es/discapacidad *[Última consulta: 25 de mayo de 2022]*
[155] CERMI., "La RAE enmienda el término "discpacidad" en el diccionario", *cermi*, 24 de noviembre de 2020, disponible en: https://www.cermi.es/es/actualidad/noticias/la-rae-enmienda-el-t%C3%A9rmino-%E2%80%98discapacidad%E2%80%99-en-el-diccionario *[Última consulta: 25 de mayo de 2022]*
[156] BOE núm. 289 de 3 de diciembre de 2013

admite que las disfunciones cambien con el tiempo, rompiendo la idea estática de la discapacidad[157].

La Ley 8/2021, objeto de estudio del presente capítulo, no define el concepto de la discapacidad. La autora GARCÍA RUBIO[158] considera que la falta de una definición del término que delimite los destinatarios de la normativa es necesaria y facilita su aplicación a cualquier tipo de característica física, psíquica o sensorial, que en interacción con la sociedad, impida o dificulte a la persona una actuación jurídica en plenas condiciones de igualdad con los demás.

2.5. La personalidad jurídica, la capacidad jurídica, la capacidad de obrar y la modificación judicial de la capacidad de obrar:

En el Código Civil se realizaba una triple distinción de tres conceptos conectados entre sí, diferenciando la personalidad jurídica, la capacidad jurídica y la capacidad de obrar, a las cuales se les sumaba el proceso de modificación de la capacidad. No es nuestra intención realizar aquí un análisis exhaustivo de los citados conceptos, pero consideramos que a efectos de definir la capacidad de las personas mayores con discapacidad, es necesario comprender qué efecto ha tenido la reforma operada por la ley 8/2021 en cada uno de los referidos conceptos.

El artículo 29 del CC establece que el nacimiento determina la personalidad, debiendo producirse el entero desprendimiento del seno materno para su reconocimiento. El derecho concede la personalidad jurídica a cada uno de los individuos humanos en cuanto que son personas[159]. Por ende, mediante la personalidad jurídica, se reconoce a los seres humanos como personas ante la Ley. Gracias a esta condición, se adquieren los derechos y deberes.

El concepto tradicional de la capacidad jurídica, como sabemos, hace referencia a la capacidad que tiene todo ser humano, desde su nacimiento por el mero hecho de serlo, no pudiendo ser suprimida, ni limitada, sino por causa de muerte. La capacidad jurídica no admite grados ni matizaciones, es igual para todas las personas. La capacidad jurídica es consustancial a la persona; por lo que, los términos de personalidad jurídica y capacidad jurídica son términos tangentes[160]. En cambio, en el Código Civil, la capacidad jurídica se diferenciaba de la capacidad de obrar, tratándose esta última de la aptitud o capacidad para realizar actos jurídicos válidos y asumir, en consecuencia,

[157] GÁRATE ITURRI, J.C., "Concepto jurídico de discapacidad", Anales de derecho y discapacidad, Núm. 6, 2021, p. 55
[158] GARCÍA RUBIO, M. P., "La reforma de la discapacidad en el Código Civil. Su incidencia en las personas de edad Avanzada", en GREGORACI FERNANÁNDEZ, B. y VELASCO CABALLERO, F. (Ed.), *El derecho de las sociedades envejecidas*, Editorial BOE, Madrid, 2021, p. 89
[159] BONILLA SÁNCHEZ, J.J., *Personas y derechos de la personalidad*, Reus, Madrid, 2010, p. 24
[160] LASARTE ÁLVAREZ, C., *Protección jurídica del menor*, Tirant lo Blanc, Valencia, 2016, p.28

derechos u obligaciones específicas, como otorgar un testamento, comparecer en concepto de testigo, intervenir en calidad de fiador o contraer matrimonio[161].

Desde esta óptica superada por la reforma, la modificación judicial de la capacidad de obrar, antigua incapacitación judicial[162], era un procedimiento judicial por el cual un juez sometía a una persona con discapacidad a un régimen especial de protección de su persona de sus bienes. Esto suponía el paso de la situación de hecho a una situación jurídica, pues implicaba una declaración judicial a través de la cual se dotaba a la persona con discapacidad de un sistema de protección concreto. La sentencia de modificación de la capacidad destruía la presunción legal de plena capacidad de obrar del mayor de edad, y dictaba qué régimen le correspondía[163]. Otra pieza del sistema, el antiguo artículo 200 del Código Civil, se encargaba de indicar las causas que producían la modificación de la capacidad; a saber, la enfermedad o deficiencia de carácter físico o psíquico, persistencia de la enfermedad o deficiencia y la imposibilidad de autogobierno. El contenido del citado artículo era lo suficientemente amplio y flexible para que cualquier anomalía física o psíquica que persistiera en el tiempo e impidiese a la persona gobernarse por sí misma pudiese ser apreciada como causa de incapacitación[164]. Aunque la discapacidad sea diversa, en el antiguo sistema casi todos los casos terminaban con la aplicación de la incapacidad total.

La doctrina ha puesto de manifiesto que en este sistema muchas personas han sido injustamente privadas del ejercicio de sus derechos. Como indica HERNÁNDEZ SÁNCHEZ ante los determinados supuestos en los que se podía encontrar una persona mayor con capacidad de obrar con dificultades para su autogobierno, la solución no podía ser la medida desproporcionada de la modificación judicial de la capacidad de obrar. La clave se encontraba en que fuesen asistidos en la toma de decisiones, respetando su autonomía de la voluntad y sus preferencias personales[165]. En el mismo sentido, GARCÍA PONS afirmaba que la incapacitación es una forma de protección ineficaz, y que no era posible que el único instrumento jurídico fuese la tradicional incapacitación judicial que equivalía a la muerte civil, siendo necesaria la introducción del sistema de apoyos[166], sistema que será analizado más adelante.

La sentencia del Tribunal Supremo de 1 de julio de 2014[167], afirmó que la incapacitación debía ser un traje a medida; para lo cual había que conocer muy bien la

[161] FERNÁNDEZ DE BUJÁN, A., "Capacidad. discapacidad. incapacidad. Incapacitación", *revista de derecho UNED*, Núm. 9, 2011, pp. 83-85

[162] La Ley 15/2015, de 2 de julio de la Jurisdicción Voluntaria, abandonó el empleo de los términos de incapaz o incapacitación, y los sustituyó por la referencia a las personas cuya capacidad está modificada judicialmente.

[163] ZURITA MARTÍN, I., *Protección civil de la ancianidad*, *cit.*, pp. 53-54

[164] GONZÁLEZ GRANDA, P., *Régimen jurídico de protección de la discapacidad por enfermedad mental*, Reus, Madrid, 2009, p. 71

[165] SÁNCHEZ HERNÁNDEZ, A., "La guarda de apoyo: propuesta para la protección de la persona mayor con discapacidad", *Revista jurídica de Castilla y León*, Núm. 44, 2018, p. 93

[166] GARCÍA PONS, A., "El artículo 12 de la Convención de Nueva York de 2006 sobre los Derechos de las Personas con Discapacidad y su impacto en el Derecho Civil de los Estados signatarios: el caso de España", *Anuario de derecho civil*, Vol. 66, Núm. 1, 2013, p. 113

[167] STS 341/2014, 1 de julio de 2014 (Rec. Núm. 341/2014), FJ.6

situación de esa concreta persona, cómo se desarrollaba su vida ordinaria y en qué medida podía cuidarse por sí misma o necesitaba alguna ayuda[168].

En la sentencia de la Audiencia Provincial de Burgos de 4 marzo 1997 (AC l997\652) se indicó que las limitaciones propias de la edad no daban lugar, necesariamente, a la modificación de la capacidad de la persona mayor, puesto que había que atender, en cada caso, a su capacidad de autogobierno. La Audiencia Provincial de Burgos, resolviendo sobre la incapacitación de una mujer de edad avanzada a solicitud del Ministerio Fiscal, revocó la sentencia estimatoria del Juzgado de Primera Instancia, al entender que la demandada no se hallaba en una situación personal que hiciese necesaria su incapacitación. El perito concluyó que la demandada era una persona con las limitaciones propias de la edad, pero en ningún momento dijo que su situación personal la impidiese regirse por sí misma, por lo que la demandada podía tomar decisiones en cuanto a su vida y patrimonio, y lo que era más importante, que su capacidad era suficiente para gobernar su vida y bienes en las condiciones y medio habitual.

En base a la Sentencia de la Audiencia Provincial de Barcelona 22 noviembre 1999 (AC 1999\8282), la concurrencia de demencia senil o de enfermedad como el Alzheimer tampoco producía, en todo caso, la incapacitación total de la persona enferma, sino que podía determinarse la incapacitación parcial de la misma si se atendía al dato de su aptitud para gobernar sus actos. La demandada padecía una demencia degenerativa primaria de tipo leve, conservaba su capacidad de autogobierno y únicamente precisaba la ayuda de otras personas a modo de asistencia, gozando de plena autonomía para desplazarse y para el gobierno de su persona. Al tener una plena autonomía a nivel funcional, el Tribunal estimó que no se podía declarar su incapacidad total. No obstante, dado que se dedujo que necesitaba una protección en el ámbito patrimonial, debía decretarse la incapacitación parcial de la misma, y nombrar un curador para que la asistiera en todos los actos de enajenación, gravamen y disposición.

3. EVOLUCIÓN LEGISLATIVA:

3.1. El artículo 12 de la Convención Internacional sobre los derechos de las personas con discapacidad de Nueva York:

Mediante resolución de 19 de diciembre de 2011, la Asamblea General de Naciones Unidas decidió establecer un Comité Especial para la creación de la Convención Internacional sobre los Derechos de las Personas con Discapacidad[169]. Dicho Comité Especial elaboró un proyecto que finalmente fue adoptado por consenso el día 13 de diciembre de 2006 en la 76ª sesión plenaria de la Asamblea General, constituyendo el

[168] El Tribunal Europeo de Derechos Humanos, en su sentencia 44009/05 de 27 de marzo de 2008, asunto Chtoukatourov contra Rusia y STEDH 33117/02, de22 de enero de 2013, asunto Lashin contra Rusia, tras observar que la Ley rusa solo recogía la plena capacidad y la incapacidad total, alegó que las legislaciones deben prever una respuesta individualizada para cada caso concreto.

[169] Resolución de la Asamblea General de Naciones Unidas 56/168, de 19 de diciembre de 2001

primer convenio internacional sobre las personas con discapacidad: La Convención Internacional sobre los derechos de las personas con discapacidad de Nueva York (la Convención o CDPD).

Por primera vez se conseguía recoger en un mismo instrumento jurídico internacional todas las grandes reivindicaciones del sector de la discapacidad, marcando un cambio paradigmático de las actitudes y enfoques respecto de las personas con discapacidad y consagrando los derechos humanos de las personas con discapacidad[170]. La CDPD fue ratificada por España el 30 de noviembre de 2007, entrando en vigor el 3 de mayo de 2008[171]. En base al artículo 96 CE, al ser un tratado internacional ratificado, este tratado se considera como fuente del Derecho español.

Aunque la CDPD se compone de cincuenta artículos, es de interés comprender la esencia del artículo 12 de la CDPD, dado que es el origen y razón de ser de la Ley 8/2021, de ahí la necesidad de realizar un conciso análisis del citado artículo para el presente trabajo. Se trata del artículo que ha impulsado el cambio de paradigma en cuanto al tratamiento de los derechos de las personas con discapacidad, por ello, cobra especial importancia dentro del CDPD. A su vez, se ha de estudiar la Observación general Nº 1 del 2014 del Comité sobre los Derechos de las Personas con Discapacidad de la Organización de Naciones Unidas (CRPD)[172], donde el citado comité realiza interpretación detallada de cada uno de los párrafos del artículo 12 de la Convención[173].

---

[170] PINDADO GALÁN, M. y MARRERO MACÍAS, R., "Desarrollos normativos derivados de la Convención sobre los derechos de las personas con discapacidad en España. Una perspectiva desde los derechos de las personas con trastorno del espectro del autismo", Confederación Autismo España, 2022, p. 8, disponible en: http://riberdis.cedd.net/handle/11181/6509 *[Última consulta: 5 de junio de 2022]*

[171] Previa a la entrada en vigor de la CDPD, en España se habían creado ciertas leyes relativas a las personas con discapacidad entre las cuales merecen especial mención: Ley 13/1982, de 7 de abril, de integración social de los minusválido; Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad; y la Ley 49/2007, de 26 de diciembre, por la que se establece el régimen de infracciones y sanciones en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad.

[172] CRPD. Observación general nº 1 (2014), de 19 de mayo de 2014

[173] Artículo 12 de la CDPD:

"1. Los Estados Partes reafirman que las personas con discapacidad tienen derecho en todas partes al reconocimiento de su ***personalidad jurídica****.*

2. Los Estados Partes reconocerán que las personas con discapacidad tienen ***capacidad jurídica*** *en igualdad de condiciones con las demás en todos los aspectos de la vida*

3. Los Estados Partes adoptarán las medidas pertinentes para proporcionar acceso a las personas con discapacidad al ***apoyo que puedan necesitar en el ejercicio de su capacidad jurídica****.*

4. Los Estados Partes asegurarán que en todas las medidas relativas al ejercicio de la capacidad jurídica se proporcionen ***salvaguardias adecuadas y efectivas*** *para impedir los abusos de conformidad con el derecho internacional en materia de derechos humanos. Esas salvaguardias asegurarán que las medidas relativas al ejercicio de la capacidad jurídica respeten los derechos, la voluntad y las preferencias de la persona, que no haya conflicto de intereses ni influencia indebida, que sean proporcionales y adaptadas a las circunstancias de la persona, que se apliquen en el plazo más corto posible y que estén sujetas a exámenes periódicos por parte de una autoridad o un órgano judicial competente, independiente e imparcial. Las salvaguardias serán proporcionales al grado en que dichas medidas afecten a los derechos e intereses de las personas.*

5. Sin perjuicio de lo dispuesto en el presente artículo, los Estados Partes tomarán todas las ***medidas que sean pertinentes y efectivas*** *para garantizar el derecho de las personas con discapacidad, en igualdad de condiciones con las demás, a ser propietarias y heredar bienes, controlar sus propios asuntos*

Bajo el título de "igual reconocimiento como persona ante la Ley", el artículo 12 CDPD reconoce en el punto primero que las personas con discapacidad tienen derecho al reconocimiento de su personalidad jurídica. Según se indica en el segundo punto del artículo objeto de análisis, los Estados Partes deben reconocerles esta capacidad jurídica en igualdad de condiciones en todos los aspectos de la vida. De esta manera, se respalda lo recogido en los artículos 1 y 6 de la Declaración Universal de Derechos Humanos[174], puesto que, en los mismos, se indica que todos los seres humanos nacen libres e iguales en dignidad de derechos, y que todo ser humano tiene derecho al reconocimiento de su personalidad jurídica.

En cuanto al punto tercero del artículo 12 CDPD, se recoge la obligación que tienen los Estados Partes de adoptar las medidas necesarias para proporcionar a las personas con discapacidad el apoyo que necesiten en el ejercicio de su capacidad jurídica[175]. Este punto adquiere especial importancia al introducir el elemento que ha provocado el cambio legislativo: el apoyo. Se rompe con el sistema tradicional de sustitución para pasar al sistema de apoyos, cuyo objetivo es asistir a las personas con discapacidad en el ejercicio de su capacidad jurídica. A su vez, las personas con discapacidad tienen la posibilidad de rechazar o no ejercer su derecho a recibir esta ayuda[176]. Bajo la ya citada rúbrica del igual reconocimiento como persona ante la ley, el artículo 12 concreta aquella genérica finalidad en una también amplia formulación del paradigma de apoyos a los que deben tener acceso las personas con discapacidad[177].

En base al punto cuarto del citado artículo, los Estados partes deben introducir salvaguardias adecuadas y efectivas para impedir que se produzcan abusos de conformidad con el derecho internacional en materia de derechos humanos a la hora de ejercer esta capacidad jurídica. Dichas salvaguardias asegurarán que las medidas relativas al ejercicio de la capacidad jurídica respeten los derechos, la voluntad y las preferencias de la persona, que no haya conflicto de intereses ni influencia indebida, que sean proporcionales y adaptadas a las circunstancias de la persona, que se apliquen en el plazo más corto posible y que estén sujetas a exámenes periódicos por parte de una autoridad o un órgano judicial competente, independiente e imparcial. Las salvaguardias deben ser proporcionales al grado en que dichas medidas afecten a los derechos e intereses de las personas. Esto es, el artículo 12.4 de la Convención recoge que las medidas de apoyo deben incluir salvaguardas, indicando a continuación cuáles han de

---

económicos y tener acceso en igualdad de condiciones a préstamos bancarios, hipotecas y otras modalidades de crédito financiero, y velarán por que las personas con discapacidad no sean privadas de sus bienes de manera arbitraria".

[174] La Declaración Universal de los Derechos Humanos es un documento adoptado por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), el 10 de diciembre de 1948 en París, que recoge en sus 30 artículos los derechos humanos básicos.

[175] La Convención no proporciona datos sobre cómo, o qué rasgos debe tener el sistema de apoyos. De esta manera, otorga a los Estados Partes un cierto margen de discrecionalidad, los cuales deben proceder a adecuar su normativa a la Convención. En este sentido: BARIFFI, F.J., *El régimen jurídico internacional de la capacidad jurídica de las personas con discapacidad*, Ediciones Cinca, Madrid, 2016, p. 365

[176] Punto 19 de la Observación general Nº 1 (2014) del CRPD

[177] IMAZ ZUBIAUR, L., "Reformulando la protección de las personas con diversidad funcional a la luz de la distante Convención de Nueva York de 2006", *Revista Vasca de Administración Pública*, Núm. 112, 2018, p. 196

ser los propósitos de estas salvaguardias, siendo el primero de ellos que las medidas de apoyo respeten los derechos, la voluntad y las preferencias de la persona[178].

La Convención arrumba el viejo edificio del sistema de incapacitación, condenando la negación de la capacidad jurídica de modo discriminatorio, y exigiendo que se proporcione apoyo en su ejercicio[179]. Los Estados partes no deben negar a las personas con discapacidad su capacidad, sino que deben proporcionarles acceso al apoyo que necesiten para tomar decisiones que tengan efectos jurídicos[180], terminando de esta forma con el sistema tradicional de sustitución en la toma de decisiones[181]. En consecuencia, la Convención colisiona con la figura de la incapacitación, como mecanismo sustitutivo de la capacidad de obrar, y obliga a adoptar una nueva herramienta basada en un sistema de apoyos que se proyecte sobre las circunstancias concretas de la persona, el acto o negocio a realiza.

Se ha dicho que la filosofía de la Convención es "acompañar sin sustituir". Se asume que una consecuencia directa del reconocimiento de la dignidad de la persona que tiene una discapacidad es la obligación de poner los medios necesarios para que, en la medida de lo posible, pueda tomar sus propias decisiones. En el desarrollo de tal objetivo, la CDPD, propugna no solo el reconocimiento de la capacidad jurídica de todas las personas, sino también en la eliminación de los sistemas que establecen el reemplazo de la voluntad de la persona con discapacidad en la toma de decisiones[182].

Tal y como se adelantaba más arriba, el apoyo en el ejercicio de la capacidad jurídica debe respetar los derechos, la voluntad y las preferencias de las personas con discapacidad y nunca debe consistir en decidir por ellas[183]. Incluso ante una situación extrema, en la que la persona con discapacidad no pueda expresar su voluntad, se deberá respetar su autonomía individual la capacidad de adoptar decisiones[184]. Esta obligación de respetar la autonomía debe traducirse en la configuración de apoyos a medida, y en el respeto a la esfera de autonomía e independencia individual que presente en orden a la articulación y desarrollo de las mismas[185]. En el caso de que, aun habiendo realizado un esfuerzo considerable no sea posible determinar la voluntad y las preferencias de una persona, la determinación del "interés superior" debe ser sustituida

[178] MARTÍNEZ-PUJALTE, A.L., "A propósito de la reforma de la legislación española en materia de capacidad jurídica: la voluntariedad como nota esencial del apoyo", *Cuadernos Electrónicos de Filosofía del Derecho*, Núm.42, 2020, pp. 246-247
[179] Punto 15 de la Observación general Nº 1 (2014) del CRPD
[180] Punto 16 de la Observación general Nº 1 (2014) del CRPD
[181] En el escrito del Ministerio Fiscal, respondido por la STS 282/2009, 29 de abril de 2009 (Rec. Núm. 1259/2006), se dice que la configuración tradicional de la incapacitación, puede suponer una limitación excesiva e incluso absoluta de la capacidad de obrar, en aquellas personas con alguna deficiencia física, intelectual o psicosocial, impidiéndoles la realización de actos de carácter personal y patrimonial o suponiendo en la práctica, un modelo de sustitución en la toma de decisiones.
[182] LEGERÉN-MOLINA, A., La relevancia de la voluntad de la persona con discapacidad en la gestión de los apoyos, pp. 166-167, en SALAS DE MURILLO, S. y MAYOR DEL HOYO, M.V (Dir)., *Claves para la adaptación del ordenamiento jurídico privado a la convención de naciones unidas en materia de discapacidad*, Tirant lo Blanch, Valencia, 2019
[183] Punto 17 de la Observación general Nº 1 (2014) del CRPD
[184] Punto 18 de la Observación general Nº 1 (2014) del CRPD
[185] STS 2018/934 de 7 de marzo de 2018 (Rec. Núm. 4192/2016)

por la "mejor interpretación posible de la voluntad y las preferencias". Gracias a esta sustitución respetuosa con la voluntad de la persona con discapacidad, se permite que disfruten del derecho a la capacidad jurídica en condiciones de igualdad que el resto de la sociedad[186].

De la lectura del artículo 12 de la Convención podemos apreciar que en todo momento se habla de capacidad jurídica, no de la capacidad de obrar. Cuando el artículo 12 de la Convención se refiere en sus dos primeros apartados a la personalidad jurídica y a la capacidad jurídica, se está refiriendo a la aptitud de toda persona de ser titular de derechos y obligaciones jurídicas, y cuando en los párrafos tercero y cuarto habla del ejercicio de la capacidad jurídica se está refiriendo a la capacidad de obrar[187].

En esta misma línea, en la Observación se afirma que el concepto de la capacidad jurídica engloba la tradicional distinción del concepto de capacidad jurídica y capacidad de obrar[188]. Más concretamente, en el punto 14 de se indica que, la capacidad jurídica tiene dos facetas. La primera es la capacidad legal de ser titular de derechos y de ser reconocido como persona jurídica ante la ley. La segunda es la legitimación para actuar con respecto a esos derechos y el reconocimiento de esas acciones por la ley, siendo el componente que frecuentemente se deniega o reduce en el caso de las personas con discapacidad. La capacidad jurídica significa que todas las personas, incluidas las personas con discapacidad, tienen la capacidad legal y la legitimación para actuar simplemente en virtud de su condición de ser humano. Por consiguiente, para que se cumpla el derecho a la capacidad jurídica deben reconocerse las dos facetas de esta; esas dos facetas no pueden separarse. De esta forma, se vuelve a subrayar que el sistema de incapacitación debe ser eliminado.

El quinto y último párrafo del artículo 12 del Convención, obliga a los Estados partes a adoptar medidas, con inclusión de medidas legislativas, administrativas y judiciales y otras medidas prácticas, para garantizar los derechos de las personas con discapacidad en lo que respecta a las cuestiones financieras y económicas, en igualdad de condiciones con las demás. El criterio de negar a las personas con discapacidad el acceso a las finanzas, debe sustituirse por el apoyo para ejercer la capacidad jurídica, de acuerdo con el analizado artículo 12.3 CDPD. Gracias a este apoyo, se permite que las personas con discapacidad sigan teniendo el control sobre sus asuntos económicos.

Teniendo en cuenta todo lo anterior, no sorprende que el Comité para los Derechos de las Personas con Discapacidad de Naciones Unidas[189], en su sesión 62ª celebrada el 23

[186] Punto 21 de la Observación general Nº 1 (2014) del CRPD

[187] SERRANO GARCÍA, I., *Autotutela: El artículo 223-II del Código Civil y la Convención de Nueva York sobre los derechos de las personas con discapacidad de 2006*, Tirant lo Blanch, Valencia, 2012, p. 24.

[188] De la misma manera, en la ya cita STS 282/2009, 29 de abril de 2009 se recoge que "la Convención unifica la capacidad jurídica y de obrar en un todo inseparable".

[189] El Comité de los Derechos de las Personas con Discapacidad (CRPD) es el órgano de expertos independientes que supervisa la aplicación de la Convención sobre los Derechos de las Personas con Discapacidad.

de septiembre de 2011[190], recomendara al Estado Español que revisase las leyes que regulaban la guarda y la tutela, y que tomase medidas para adoptar leyes y políticas por las que se reemplazaran los regímenes de sustitución en la adopción de decisiones por una asistencia para la toma de decisiones que respetase la autonomía, la voluntad y las preferencias de la persona. Posteriormente, en el Informe elaborado por el Comisario para los Derechos Humanos del Consejo de Europa tras su visita a España, del 3 al 7 de junio de 2013, se instaba a las autoridades a concluir, como objetivo prioritario, el proceso de reforma de la legislación relativa a la capacidad jurídica de las personas con discapacidad intelectual y psicosocial, dando pleno efecto a los principios consagrados en la Convención. A su vez, se indicaba que dicho proyecto de ley debía de haberse adoptado en el transcurso de un año tras la adopción de la Ley 26/2011 de 1 de agosto, de adaptación normativa a la Convención Internacional sobre los Derechos de las Personas con Discapacidad[191]. La incorporación de la Convención al ordenamiento jurídico estatal requería una gran reforma normativa, debiendo modificar o derogar todas las normas que fueran contrarias a la Convención[192]; y es que, el artículo 12 CDPD afectaba a principios y conceptos plenamente arraigados como la plena capacidad o la validez y los vicios del consentimiento[193].

3.2.Las reformas posteriores a la adopción de la Convención:

Tras la ratificación de la Convención, se produjeron reformas legislativas que han tratado de adaptar parcialmente el ordenamiento jurídico estatal al espíritu de la Convención. Dentro de este grupo de normas, destacaremos las que merecen una mención especial en relación con las personas mayores con discapacidad con el objetivo de comprender el camino que se ha seguido para llegar a la Ley 8/2021, y los cambios, tanto legales como sociales, que se han producido en el proceso.

El primer paso se dio mediante la Ley 1/2009, de 25 de marzo[194], de reforma de la Ley de 8 de junio de 1957 sobre el Registro Civil[195], en materia de incapacitaciones, cargos tutelares y administradores de patrimonios protegidos, y de la Ley 41/2003, de 18 de noviembre, sobre protección patrimonial de las personas con discapacidad y de

[190] CRPD. Examen de los informes presentados por los Estados partes en virtud del artículo 35 de la Convención: Observaciones finales del Comité sobre los Derechos de las personas con Discapacidad, 19 de octubre de 2011
[191] COMISARIO PARA LOS DERECHOS HUMANOS DEL CONSEJO DE EUROPA. Informe tras su visita a España del 3 al 7 de junio de 2013, pp. 28-31
[192] VIVAS-TESÓN, I., "Retos actuales en la protección jurídica de la discapacidad", *Pensar-Revista de Ciências Jurídicas*, Vol. 20, Núm. 3, 2015, p. 833
[193]GUILARTE MARTÍN-CALERO, C., "Algunas consideraciones sobre el consentimiento de las personas con discapacidad mental e intelectual", *Revista Doctrinal Aranzadi Civil-Mercantil*, Núm. 11, 2018, p. 141
[194] BOE núm. 73, de 26 de marzo de 2009
[195] BOE núm. 151, de 10 de junio de 1957

modificación del Código Civil, de la Ley de Enjuiciamiento Civil de la normativa tributaria con esta finalidad[196].

En cuanto a la Ley 18/2011, de 5 de julio, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia[197]; en su preámbulo se afirmaba que, todas las personas tienen derecho a obtener la tutela efectiva de sus derechos ante los tribunales, y que para salvaguardar dichos derechos era necesaria la modernización de la Administración de Justicia[198].

Posteriormente, entro en vigor una de las normas clave para este cambio, nos referimos a la Ley 26/2011[199], de 1 de agosto, de adaptación normativa a la Convención de Derechos de las Personas con Discapacidad[200]. De la mano de la Ley 26/2011, se adoptó el Real Decreto 1276/2011, de 16 de septiembre de adaptación normativa a la Convención Internacional sobre los derechos de las personas con discapacidad[201]. El objetivo de este Real Decreto, era adecuar la regulación reglamentaria en materia de discapacidad a las directrices de la Convención, en la línea de lo marcado por la Ley 26/2011[202].

Pronto se manifestó la necesidad de elaborar un Texto Refundido previsto en la disposición final segunda de la Ley 26/2011, en el que se regularizasen, aclarasen y armonizasen el conjunto de normas referido a las circunstancias en cuestión, a saber, la Ley 13/1982, de 7 de abril, de integración social de los minusválidos, la Ley 51/2003, de 2 de diciembre, de igualdad de oportunidades, no discriminación y accesibilidad

[196] Su Disposición Final Primera requería al Gobierno que, en el plazo de seis meses desde la entrada en vigor de esta Ley, remitiera a las Cortes Generales un Proyecto de Ley de reforma de la legislación reguladora de los procedimientos de incapacitación judicial, que pasaría a denominarse procedimientos de modificación de la capacidad de obrar, para su adaptación a las previsiones de la Convención, aunque no se logró dicho objetivo.

[197] BOE núm. 160, de 6 de julio de 2011

[198] En su Disposición adicional cuarta, relativa a la accesibilidad a los servicios electrónicos, se exigía a las Administraciones con competencias en materia de justicia garantizar que todos los ciudadanos, con especial atención a las personas mayores o con algún tipo de discapacidad, que se relacionasen con la Administración de Justicia pudiesen acceder a los servicios electrónicos en igualdad de condiciones con independencia de sus circunstancias personales, medios o conocimientos. Al mencionar expresamente a las personas mayores, la normativa habla de una forma indirecta de la brecha digital que ha sido analizada anteriormente en este trabajo.

[199] BOE núm. 184, de 2 de agosto de 2011

[200] En la Disposición adicional séptima, se exigía al Gobierno que, en el plazo de un año a partir de la entrada en vigor de la Ley, remitiera a las Cortes Generales un proyecto de ley de adaptación normativa del ordenamiento jurídico para dar cumplimiento al artículo 12 de la Convención, en lo relativo al ejercicio de la capacidad jurídica por las personas con discapacidad en igualdad de condiciones que las demás en todos los aspectos de la vida. Dicho proyecto de ley debía establecer las modificaciones necesarias en el proceso judicial de determinación de apoyos para la toma libre de decisiones de las personas con discapacidad que lo precisasen. No obstante, no se realizo dicho proyecto de ley en el tiempo requerido.

[201] BOE núm. 224, de 17 de septiembre de 2011

[202] En materia de protección civil, la modificación consistía en garantizar la asistencia en general de las personas con discapacidad; regular protocolos de actuación específicos; así como incluir en los cursos de formación materias relacionadas con la asistencia a personas con discapacidad. En materia de sanidad, los cambios realizados estaban dirigidos a garantizar el derecho de acceso a la información de las personas con discapacidad, previendo la utilización de formatos adecuados y el apoyo en la prestación de consentimiento de las personas con discapacidad.

universal de las personas con discapacidad y la Ley 49/2007, de 26 de diciembre, de infracciones y sanciones en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad. Así, se aprobó el Real Decreto Legislativo 1/2013, de 29 de noviembre, por el que se aprueba el Texto Refundido de la Ley General de derechos de las personas con discapacidad y de su inclusión social[203], que refundía las citadas normas.

Dos años más tarde, se aprobó la Ley 15/2015, de 2 de julio, de modificación de la Ley de Jurisdicción Voluntaria[204]. Como indica en el preámbulo, mediante esta Ley se buscaba la adaptación a la Convención, abandonando el empleo de los términos de incapaz o incapacitación, los cuales se sustituyen por la referencia a las personas cuya capacidad está modificada judicialmente.

En cuanto a la Ley Orgánica 2/2018, de 5 de diciembre, para la modificación de la Ley Orgánica 5/1985, de 19 de junio[205], del Régimen Electoral General para garantizar el derecho de sufragio de todas las personas con discapacidad, se manifestaba que la regulación del derecho de sufragio anterior a esta Ley Orgánica chocaba con el principio de igualdad ante la ley consagrado en la Constitución, puesto que, dentro de los apartados b) y c) del artículo 3.1 de la antigua Ley Orgánica se disponía que carecían de derecho de sufragio los declarados incapaces en virtud de sentencia judicial firme, siempre que la misma declarase expresamente la incapacidad para el ejercicio del derecho de sufragio[206]; y los internados en un hospital psiquiátrico con autorización judicial, durante el período que durase su internamiento siempre que en la autorización el juez declarase expresamente la incapacidad para el ejercicio del derecho de sufragio[207].

---

[203] BOE núm. 289, de 3 diciembre de 2013.

[204] BOE núm. 158, de 3 de julio de 2015. Bajo el título de "respeto a la autonomía de las personas con discapacidad", el artículo 6 del Real Decreto indica que el ejercicio de los derechos de las personas con discapacidad debe realizarse de acuerdo con el principio de libertad en la toma de decisiones. Las personas con discapacidad tienen derecho a la libre toma de decisiones, para lo cual la información y el consentimiento deben efectuarse en formatos adecuados y de acuerdo con las circunstancias personales, siguiendo las reglas marcadas por el principio de diseño universal o diseño para todas las personas, de manera que les resulten accesibles y comprensibles. El citado artículo termina indicando que, se deben tener en cuenta las circunstancias personales del individuo, su capacidad para tomar el tipo de decisión en concreto y asegurar la prestación de apoyo para la toma de decisiones.

[205] BOE núm. 294, de 6 de diciembre de 2018

[206] La sentencia del TEDH caso Alajos Kiss contra Hungría de 20 de mayo de 2010 (demanda n. 38832/06), consideró que se había producido una violación del artículo 3 del Protocolo nº 1 del Convenio por privar del derecho a voto a una persona diagnosticada un síndrome maníaco-depresivo con capacidad modificada judicialmente y sometida a curatela.

[207] Ante esta exclusión, el Comité sobre los derechos de las personas con discapacidad de Naciones Unidas, en su 62.ª sesión celebrada el 23 de septiembre de 2011, recomendó que se revisase toda la legislación pertinente para que todas las personas con discapacidad, independientemente de su deficiencia, de su condición jurídica o de su lugar de residencia, tuviesen derecho a votar y a participar en la vida pública en pie de igualdad con los demás. Así lo manifestaba también GUILARTE-MARTIN CALERO, quien previa a la Ley Orgánica 2/2018, indicaba que sería deseable que el legislador reformara el artículo 3 de la LRED y no conectara la privación del derecho de voto al proceso de modificación de la capacidad de obrar; dado que esta medida ni protegía a la persona con discapacidad ni evitaba un perjuicio a la sociedad. Véase en este aspecto: GUILARTE MARTÍN-CALERO, C., "La reinterpretación jurisprudencial de los sistemas de protección a la luz de la convención de Nueva York: El nuevo

Finalmente, y como instrumento que produce la adecuación plena de la normativa al artículo 12 de la Convención, se aprobó la Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica[208]. En cuanto al procedimiento legislativo, en marzo de 2018, se remitió la Propuesta de Anteproyecto de Ley al Ministerio de Justicia, siendo aprobada seis meses después, el 21 de septiembre de 2018 por el Gobierno. Dos años más tarde, el 7 de julio de 2020, se aprobó el proyecto de Ley, y habiendo publicado el Proyecto en el Boletín Oficial de las Cortes el 17 de julio, fue aprobado en la Comisión de Justicia del Congreso de los Diputados el 21 de marzo de 2021. Tras su entrada en el Senado, se aprobó por el Pleno del Senado el 12 de mayo de 2021, y se remitió al Congreso de los Diputados. El 3 de junio se promulgó en el BOE como la Ley 8/2021, de 2 junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica, y entró en vigor el 3 de septiembre de 2021[209]. Por ende, han tenido que transcurrir catorce años para que se produzca la adecuación del Derecho Civil estatal al artículo 12 de la Convención.

3.3.Principales cambios operados por la reforma:

En palabras de ZURITA MARTÍN la Ley 8/2021 se trata de una reforma largamente esperada y de todo punto necesaria, puesto que es el vehículo de adaptación del ordenamiento español a la Convención[210]. Es una de las reformas más profundase impactantes en materia de derecho privado, que afecta a multitud de artículos repartidos en nueve leyes[211] (el Código Civil, Ley de Enjuiciamiento Civil, la Ley de Jurisdicción Voluntaria, la Ley Hipotecaria, el Código Penal, la Ley de Registro Civil, la Ley del Notariado, la Ley de protección patrimonial de las personas con discapacidad y el Código de Comercio) [212].

---

paradigma de la sala primera", en GUILARTE MARTÍN-CALERO, C. y GARCÍA MEDINA, J., *Estudios y comentarios jurisprudenciales sobre discapacidad*, Aranzadi, 2016, p. 93

[208] BOE núm. 132, de 3 de junio de 2021

[209] GARCÍA RUBIO, M.P., "La reforma de la discapacidad en el Código Civil. Su incidencia en las personas de edad Avanzada", *cit.*, pp. 86-87

[210] ZURITA MARTÍN, I., "La esperada y necesaria reforma del Código Civil en materia de personas con discapacidad", *Revista de Estudios Jurídicos y Criminológicos*, Núm. 3, 2021, p. 13

[211] Es interesante visualizar mediante una tabla comparativa cómo han sido modificados estos artículos. Véase al respecto: ILUSTRE COLEGIO DE ABOGADOS DE MADRID., "Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica: cuadro comparativo", *web.icam*, 7 de junio de 2021, disponible en: https://web.icam.es/informacion-de-interes-profesional-cuadros-comparativos-con-las-modificaciones-introducidas-por-la-ley-8-2021-de-2-de-junio-y-por-la-ley-organica-8-2021-de-4-de-junio/ *[Última consulta: 10 de junio de 2022]*

[212] Como crítica se ha afirmado que carece de sentido desarrollar una prolija y abundante normativa y no dotarla de recursos, no instrumentalizar medios para que se formalice y lleve al efecto el cambio, manifestando que es necesaria igualmente una especialización en el orden jurisdiccional civil que incluya la sensibilización de la materia a tratar por los profesionales. Véase al respecto: TORTAJADA CHARTÍ, P., "La patria potestad prorrogada y la patria potestad rehabilitada en el nuevo proyecto de Ley de

En este punto nos centraremos en la modificación de los artículos del Código Civil que incumbe a las personas mayores de edad con discapacidad. Entre las novedades destacan la supresión de la modificación de la capacidad y las tradicionales instituciones de protección, y el establecimiento de las medidas de apoyo[213].

Siguiendo la línea marcada por el CDPD[214], en el Código Civil se sustituye el modelo médico o rehabilitador de atención a la discapacidad por un modelo social. En cuanto al primero, considera la discapacidad como un problema centralmente individual, que tiene su origen en las "limitaciones" de la persona originadas por el "padecimiento" de una deficiencia. Aunque reconoce a todas las personas con discapacidad la capacidad, permite y justifica la introducción de importantes restricciones y limitaciones en la capacidad de ejercicio de los derechos. En consecuencia, desde la óptica del enfoque médico, se identifica al sistema de sustitución en la toma de decisiones como pieza imprescindible del tratamiento de la capacidad jurídica[215]. Por su parte, el modelo social asume una mirada "desde" los derechos porque considera que las limitaciones que las personas con discapacidad padecen para participar plenamente en la vida social no son ni naturales, ni inevitables, ni tolerables, sino el producto de una construcción social y de relaciones de poder que constituyen una violación de su dignidad intrínseca[216].

Esta visión social entiende la discapacidad en función de su contraposición con las barreras sociales que la misma encuentra, de modo que las consecuencias jurídicas serán mayores cuando mayores sean las barreras que le impiden su inclusión social, cuando más es negada su condición de persona y se hace más énfasis en las dificultades que en las habilidades. Y por el contrario, las consecuencias serán menores cuando se facilite su concepción como persona, cuando más se consideren sus facultades, y cuando menores sean las barreras que le impidan el ejercicio de sus derechos[217]. A partir de

---

reformas de la legislación civil y procesal para el apoyo a las personas con discapacidad (actual Ley 8/2021)", *Revista Boliviana de Derecho*, Núm. 32, 2021, p. 248

[213] BESCANSA MIRANDA, R., *Protección jurídica de la persona: estudio práctico de los negocios jurídicos inter vivos y mortis causa tras la reforma de la ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica*, Aferre, Barcelona, 2021, p. 32

[214] Así lo afirma la STS Sala de lo Civil 372/2014 de 7 de julio de 2014 (Rec. Núm. 2103/2014): "*la Convención sustituye el modelo médico de la discapacidad por un modelo social y de derecho humano que al interactuar con diversas barreras, puede impedir la participación plena y efectiva del incapacitado en la sociedad, en igualdad de condiciones con las demás. Estamos ante una nueva realidad legal y judicial y uno de los retos de la* Convención *será el cambio de las actitudes hacia estas personas para lograr que los objetivos del Convenio se conviertan en realidad*".

[215] En este sentido se ha indicado que la configuración tradicional de la incapacitación, desde una concepción que tiene como base el modelo médico, puede suponer una limitación excesiva o incluso absoluta de la capacidad de obrar, en aquellas personas con alguna deficiencia física, intelectual o psicosocial, impidiéndoles la realización de actos de carácter personal y patrimonial o suponiendo en la práctica, un modela de sustitución en la toma de decisiones. Véase: FERNÁNDEZ DE BUJÁN, A., *La reforma de la jurisdicción voluntaria*, Dykinson, Madrid, 2016, pp.238-239

[216] CUENCA GÓMEZ, P., *La capacidad jurídica de las personas con discapacidad: el art. 12 de la Convención de la ONU y su impacto en el ordenamiento jurídico español*, Dykinson, Madrid, 2011, pp. 231-235

[217] RECOVER BALBOA, T., "Hacia la reforma del Código Civil y la Ley de Enjuiciamiento Civil en materia de discapacidad", en: GARCÍA GARNICA, María del Carmen y ROJO ÁLVAREZ-

esta interpretación se admite que la discapacidad tiene su origen en causas sociales, esto es, en la manera en la que está organizada la sociedad, y en sus limitaciones para que las necesidades de las personas con discapacidad sean adecuadamente atendidas[218]. Partiendo de la premisa de que toda vida humana es igualmente digna, desde este modelo social se sostiene que lo que puedan aportar a la sociedad las personas con discapacidad se encuentra íntimamente relacionado con la inclusión y la aceptación de la diferencia[219]. Por ello, en el caso de que la discapacidad impida a la persona ser autónoma e independiente, se procurará un apoyo que respete sus derechos, deseos y preferencia y sea conforme con la voluntad individual del discapacitado, ajustándose a las circunstancias y necesidad de cada sujeto[220].

Según SÁNCHEZ HERNANDEZ la piedra angular de la modificación es la capacidad jurídica consiste en la desaparición de la clásica dicotomía entre capacidad jurídica y capacidad de obrar. A la persona con discapacidad se le reconocen las dos facetas de la capacidad que hasta ahora se regían por baremos independientes: la capacidad jurídica y la capacidad de obrar. Y es que, el concepto de capacidad jurídica que recoge la Ley 8/2021, incluye tanto la aptitud de una persona para adquirir derechos y contraer obligaciones por sí misma, como la aptitud para ejercer los mismos. En el ejercicio de esta capacidad, en caso de que sea necesario, se acudirá a las medidas de apoyo pero no se modificará su capacidad jurídica bajo ningún precepto[221]. Por su parte, DE VERDA Y BEAMONTE ha manifestado su posición contraria a abandonar una distinción que tiene, según el autor, perfiles claros y ha sido unánimemente aceptada por la doctrina y la jurisprudencia[222].

En el mismo sentido, CABRA DE LUNA afirma que se abandona un sistema tradicionalmente paternalista en el que la regla general era la sustitución en la toma de decisiones que afectaban a la persona con discapacidad, por un sistema nuevo, basado en el respeto a la dignidad, voluntad y autonomía de la persona, en el que la clave reside en el concepto de "apoyos", instrumentos de ayuda, de colaboración, que van a permitir garantizar que la persona se exprese y decida conforme a su voluntad y preferencias,

---

MANZANEDA, R., *Nuevas perspectivas del tratamiento jurídico de la discapacidad y la dependencia*, Dykinson, Madrid, 2014, p. 20

[218] CUESTA, J.L.; DE LA FUENTE, R. y ORTEGA, T., "Discapacidad intelectual: una interpretación en el marco del modelo social de la discapacidad", *Controversias y Concurrencias Latinoamericanas*, Vol. 10, Núm. 18, 2019, p. 88

[219] PALACIOS, Agustina. El modelo social de discapacidad: orígenes, caracterización y plasmación en la Convención Internacional sobre los Derechos de las Personas con Discapacidad, Cinca, 2008, Madrid, p. 104

[220] FERNÁNDEZ GONZÁLEZ, M.B., *Sistema de apoyos para personas con discapacidad. Medidas jurídico-civiles y sociales*, Dykinson, Madrid, 2021, p. 24

[221] SÁNCHEZ HERNÁNDEZ, A., "Consideraciones sobre la reforma de la legislación civil en materia de discapacidad: de la incapacitación al apoyo", Redur, Núm. 19, 2021, p. 32

[222] DE VERDA Y BEAMONTE, J.R., "¿Es posible seguir distinguiendo entre capacidad jurídica y capacidad de obrar?", *Instituto de Derecho Iberoamericano*, 30 de septiembre de 2021, disponible en: https://idibe.org/tribuna/posible-seguir-distinguiendo-capacidad-juridica-capacidad-obrar/ *[Última consulta: 12 de junio de 2022]*

con plenas consecuencias tanto personales como jurídicas[223]. Este sistema de apoyos cobra especial importancia en el caso de las personas mayores con discapacidad, puesto que permitirá que no sean incapacitadas y que, con el apoyo que necesiten, puedan seguir siendo las dueñas de sus vidas[224].

No se trata de que el tercero que apoya sustituya a la persona con discapacidad, sino de que ponga a disposición de ésta su apoyo para que pueda tomar sus propias decisiones. En otras palabras, la intervención del tercero que apoya va dirigida a ayudar a ésta a decidir, acompañándola en la decisión, decidiendo con la persona y para la persona con discapacidad[225]. Se adoptarán las medidas de apoyo que sean necesarias y que responderán a lo que necesita realmente esa persona discapacitada para ejercer su capacidad jurídica, respetando sus deseos y preferencias, quedando limitada la actuación de un tercero en representación a las situaciones excepcionales que lo justifiquen[226].

Las medidas abarcaran diversas actuaciones, desde el acompañamiento amistoso y el consejo hasta la toma de decisiones, únicamente cuando no sea posible otra forma de ayuda[227]. La nueva regulación tiene como principal finalidad adecuar ese apoyo a las necesidades de la persona con discapacidad, de manera que exista una correlación entre ayuda y necesidad de ayuda, entre grado de discapacidad y grado de asistencia, y con ello se respete, al máximo posible, la autonomía, la voluntad y las preferencias de la persona con discapacidad[228]. La pregunta que se plantea por tanto, ya no es si una persona tiene la capacidad para ejercer su capacidad jurídica, sino qué tipos de apoyo necesita para ejercer dicha capacidad[229].

Desaparecen figuras civiles que hasta ahora contaban con amplio arraigo social, como la tutela y la patria potestad prorrogada o rehabilitada, las cuales se mantienen exclusivamente para los supuestos de minoría de edad. En su lugar, se introduce la

---

[223] CABRA DE LUNA, M.A., "La Reforma del Derecho Civil a la luz de la Convención de Nueva York: el rol de la Comisión de Legislación del Real Patronato sobre Discapacidad", *Revista Española de Discapacidad*, Vol. 9, Núm. 2, 2021, p. 184

[224] En este sentido, ARROYO AMAYUELAS, previa a la entrada en vigor de la reforma, y en relación a la institución catalana de *"l'assistència"* afirmaba que *"la institución es especialmente idónea para las personas que, por razón de edad, son frágiles y vulnerables y ya no pueden gobernarse completamente de forma autónoma. Debería ser una institución llamada a generalizarse, mucho más si se tiene en cuenta que, en el terreno de la protección de adultos con déficits de entendimiento, la legislación europea y supranacional sugiere que tanto la incapacitación como la tutela deberían ser desterradas de los ordenamientos jurídicos".* Véase al respecto: ARROYO AMAYUELAS, E., "El deterioro cognitivo en la vejez. Entre la vulnerabilidad y la discapacidad", *Revista de Bioética y Derecho*, Núm. 45, 2019, p. 142

[225] SÁNCHEZ HERNÁNDEZ, A., Consideraciones sobre la reforma de la legislación civil en materia de discapacidad: de la incapacitación al apoyo", *cit.*, pp. 46-47

[226] DE AMUNÁTEGUI RODRÍGUEZ, C., "El protagonismo de la persona con discapacidad en el diseño y gestión del sistema de apoyo", en: SALAS MURILLO, S. y MAYOR DEL HOYO, M.V. (dir)., *Claves para la adaptación del ordenamiento jurídico privado a la Convención de Naciones Unidas en materia de discapacidad*, Tirant lo Blanch, Valencia, 2019, p. 125

[227] SALAZAR VARELLA, C.E., *El proceso de incapacitación*, Tirant lo Blanch, Valencia, 2021, p. 345

[228] PAU PEDRÓN, A., "La reforma de las instituciones de protección", *OTROSÍ: Revista del Colegio de Abogados de Madrid*, Núm. 8, 2021, p. 39

[229] BACH, M. y KERZNER, L., "A New Paradigm for Protecting Autonomy and the Right to Legal Capacity", *lco-cdo*, 2010, p. 58, dispnible en: https://www.lco-cdo.org/wp-content/uploads/2010/11/disabilities-commissioned-paper-bach-kerzner.pdf *[Última consulta: 14 de junio de 2022]*

obligación por parte de los poderes públicos de prestar un sistema de apoyos, personalizados y adaptados a lo que necesite la persona para poder tomar sus decisiones de forma libre y autónoma[230]. Todas estas medidas adoptadas deben ser revisadas periódicamente, con el plazo máximo de tres años, o excepcionalmente seis. En este punto se ha criticado la idea de que los tribunales estén realmente preparados para crear un sistema de apoyos individualizado, en atención a las características de cada individuo, y no generalizado[231].

Las medidas de apoyo se clasifican en voluntarias (poderes y mandatos preventivos y autocuratela), judiciales (curatela y defensor judicial) y un tercer grupo al que pertenece la guarda de hecho. De entre estas medidas, la reforma otorga una especial importancia a la curatela, puesto que, el propio significado de la palabra curatela (cuidado), revela la finalidad de la institución: asistencia, apoyo, ayuda en el ejercicio de la capacidad jurídica; por tanto, como principio de actuación y en la línea de excluir en lo posible las actuaciones de naturaleza representativa, la curatela será, primordialmente, de naturaleza asistencial. Mediante esta rehabilitación de la voluntad de la persona con discapacidad, la nueva Ley hace de la autodeterminación de la persona con discapacidad el eje de su actuación en la vida jurídica[232].

La representación, regla básica del antiguo sistema, pasa ahora a ser la excepción, aplicándose exclusivamente a los casos en los que la persona con discapacidad no pueda exteriorizar su voluntad y dicha voluntad no pueda ser reconocida de otra manera. Salvo en estos supuestos, no se podrá sustituir a la persona con discapacidad en su toma de decisiones, la cual podrá valerse de los apoyos que sean precisos para formar y exteriorizar su voluntad tanto ante los juzgados como en notarías y otras instituciones públicas[233]. En este sentido, VELILLA ANTOLÍN crítica la reforma, indicando que, para eludir el mantenimiento de la tutela en los casos de personas cuya grave discapacidad psíquica les impide el autogobierno, el legislador se ha visto en la obligación de forzar o torsionar las instituciones jurídicas obviando la realidad física. Según indica, se ha preferido desvirtuar la figura de la curatela hasta eliminar su esencia en aras a evitar la indignidad que supone estar bajo la tutela de un familiar[234]. Otros autores como ARNAU MOYA van más allá, afirmando que en los casos extremos no cabe ni tan siquiera una curatela representativa puesto que no existe voluntad alguna que complementar. De modo que cuando se tiene que representar a la persona con

[230] CABRA DE LUNA, M.A., "La Reforma del Derecho Civil a la luz de la Convención de Nueva York: el rol de la Comisión de Legislación del Real Patronato sobre Discapacidad, *cit.*, p. 185

[231] BOZA RUCOSA, M., "Comentario crítico a la Ley 8/2021", *Bozarucosa*, disponible en: https://bozarucosa.com/blog/comentario-critico-a-la-ley-8-2021/ *[Última consulta: 14 de junio de 2022]*

[232] ÁLVAREZ ROYO-VILLANOVA, S., "Voluntad y consentimiento informado en la Ley para el apoyo a las personas con discapacidad", *El notario del siglo XXI: revista del Colegio Notarial de Madrid*, Núm. 100, 2021, p. 76

[233] CERMI., "El impacto de la reforma del derecho civil", *riberdis*, 2021, p. 3, disponible en: http://riberdis.cedid.es/handle/11181/6457

[234] VELILLA ANTOLÍN, N., "Una visión crítica a la Ley de apoyo a las personas con discapacidad", *El notario del siglo XXI*, 2022, disponible en: https://www.elnotario.es/opinion/opinion/10938-una-vision-critica-a-la-ley-de-apoyo-a-las-personas-con-discapacidad *[Última consulta: 16 de junio de 2022]*

discapacidad prácticamente en todos sus actos jurídicos el mecanismo adecuado sería el de la tutela[235].

La transición al nuevo sistema no va a ser sencilla, pues es razonable pensar que, por al menos a corto plazo, la toma de decisiones por parte de las personas con discapacidad en ciertas esferas de su vida se va a tener que seguir enfrentando a cuestionamientos, prejuicios y estigmatizaciones. En nuestra opinión, la sociedad debe cambiar la forma de ver a las personas con discapacidad, considerando no solo lo que pueden hacer sino lo que pueden llegar a hacer[236].

3.4.De la sustitución al apoyo:

3.4.1. El concepto de "apoyo":

Todos los seres humanos recurrimos a apoyos de diversa índole en nuestro día a día. No nos valemos por nosotros mismos para todo sino que solicitamos asesoramiento jurídico, un consejo para tomar decisiones relevantes, utilizamos herramientas mecánicas que nos faciliten el trabajo o nos permitan realizar operaciones básicas como ver, caminar, etc. La necesidad de introducir estos apoyos se gradúa en función de la complejidad del asunto, de los conocimientos, aptitudes y habilidades que se poseen[237].

Por tanto la idea de apoyo no se es una figura retórica de creación jurídica, sino una realidad social a la que el derecho civil confiere sustantividad para los casos en que sea necesario que los apoyos sean formales para actuar en la vida jurídica[238]. De esta manera, este concepto extrajurídico pasa al mundo jurídico-privado.

El término "apoyo" abarca diversos tipos de actuaciones, desde el acompañamiento amistoso, el consejo, la ayuda en la comunicación para realizar declaraciones de voluntad o la representación únicamente para aquellos casos concretos donde el apoyo no pueda darse de otro modo, tanto en la esfera patrimonial como en lo relativo a la vida ordinaria y personal, potenciando la institución de la curatela[239]. En definitiva, estos apoyos se podrán articular en los distintos aspectos de la vida, tanto personales como económicos y sociales[240] para procurar una normalización de la vida de las personas con

[235] ARNAU MOYA, F., "Aspectos polémicos de La ley 8/2021 de medidas de apoyo a las personas con discapacidad", *Revista Boliviana de Derecho*, Núm. 33, 2022, p. 565

[236] CABRA DE LUNA, M.A., "La Reforma del Derecho Civil a la luz de la Convención de Nueva York: el rol de la Comisión de Legislación del Real Patronato sobre Discapacidad", cit., p. 187

[237] LEGERÉN-MOLINA, A., "La relevancia de la voluntad de la persona con discapacidad en la gestión de los apoyos", en: SALAS DE MURILLO, S. y MAYOR DEL HOYO, M. V. (Dir)., *Claves para la adaptación del ordenamiento jurídico privado a la convención de naciones unidas en materia de discapacidad*, Tirant lo Blanch, Valencia, 2019, p. 180

[238] CASTRO-GIRONA MARTINEZ, A., "La reforma civil de la Ley 8/2021: el paradigma de los apoyos y el ejercicio de derechos en condiciones de igualdad", *Hay derecho*, 29 de junio de 2021, disponible en: https://www.hayderecho.com/2021/06/29/la-reforma-civil-de-la-ley-8-2021-el-paradigma-de-los-apoyos-y-el-ejercicio-de-derechos-en-condiciones-de-igualdad/ *[Última consulta: 18 de junio de 2022]*

[239] Punto 3 del preámbulo de la Ley 8/2021

[240] En este sentido, el Punto 17 de la Observación general Nº 1 (2014) del CRPD recoge que, el apoyo puede incluir, por ejemplo, la exigencia de que las entidades privadas y públicas, como los bancos y las

discapacidad. El fin consiste en evitar una vulneración sistemática de los derechos y procurar una participación efectiva en la sociedad de las personas con discapacidad, pasando de un régimen de sustitución en la adopción de decisiones a otro basado en el apoyo para tomarlas, que reconoce a estas personas como iguales ante la ley, con capacidad jurídica en todos los aspectos de la vida, y en igualdad de condiciones con los demás[241].

Puesto que la discapacidad es una condición que reviste manifestaciones muy variadas, siguiendo la idea del "traje a medida"[242] y gracias a la adaptabilidad de los apoyos, la ley quiere que se establezcan las ayudas que sean necesarias teniendo en cuenta la situación y autonomía de cada persona con discapacidad. El apoyo puede afectar tanto a la esfera personal de quien lo precise (aspectos médicos, domicilio, correspondencia, relaciones afectivas, derechos de la personalidad, etc.), a la estrictamente patrimonial (contratos, disposiciones a causa de muerte, propiedad, etc.), o ambas. A su vez, el nuevo artículo 249.1 CC dispone que las medidas de apoyo deberán ajustarse a los principios de necesidad y proporcionalidad. El primero implica que las medidas de apoyo no podrán exceder de lo que precisa la persona con discapacidad, mientras que el segundo supone que han de ser suficientes para que con ese apoyo pueda ejercer su capacidad jurídica en plenitud de condiciones[243]. Los planes de medidas de apoyo deben responder a la situación y necesidades concretas de la persona beneficiaria, personalizándose tanto las aéreas de asistencia como la figura de apoyo en cada caso, lo cual evidencia que no pueden existir modelos de planes de medidas de apoyo, deben ser creados "desde cero" para cada beneficiario[244].

Como se ha dicho más arriba, las medidas de apoyo se dividen en dos principales grupos principales: las voluntarias y las judiciales. A estos dos grupos se les suma la

---

instituciones financieras, proporcionen información en un formato que sea comprensible u ofrezcan interpretación profesional en la lengua de señas, a fin de que las personas con discapacidad puedan realizar los actos jurídicos necesarios para abrir una cuenta bancaria, celebrar contratos o llevar a cabo otras transacciones sociales. El apoyo también puede consistir en la elaboración y el reconocimiento de métodos de comunicación distintos y no convencionales, especialmente para quienes utilizan formas de comunicación no verbales para expresar su voluntad y sus preferencias.

[241] STS Sala de lo Civil 373/2016, de 3 de junio de 2016 (Rec. Núm. 2367/2015)

[242] La STS Sala de lo Civil 341/2014 de 1 de julio de 2014 (Rec. Núm. 1365/2012), introdujo el concepto del "traje a medida", afirmando que "la incapacitación no es algo rígido, sino flexible, en tanto que debe adaptarse a la concreta necesidad de protección de la persona afectada por la incapacidad, lo que se plasma en la graduación de la incapacidad. Esta graduación puede ser tan variada como variadas son en la realidad las limitaciones de las personas y el contexto en que se desarrolla la vida de cada una de ellas". Para coser este traje a medida "hay que conocer muy bien la situación de esa concreta persona, cómo se desarrolla su vida ordinaria y representarse en qué medida puede cuidarse por sí misma o necesita alguna ayuda; si puede actuar por sí misma o si precisa que alguien lo haga por ella, para algunas facetas de la vida o para todas, hasta qué punto está en condiciones de decidir sobre sus intereses personales o patrimoniales, o precisa de un complemento o de una representación, para todas o para determinados actuaciones". En mismos sentido: STS Sala de lo Civil 244/2015 de 13 de mayo de 2015 (Rec. Núm. 846/2014).

[243] GARCÍA RUBIO, M.P., "Las medidas de apoyo de carácter voluntario, preventivo o anticipatorio", *Revista de Derecho Civil*, Vol. 5, Núm. 3, 2018, p. 34

[244] CUENCA GÓMEZ, P., "El sistema de apoyo en la toma de decisiones desde la Convención Internacional sobre los Derechos de las Personas con Discapacidad: principios generales, aspectos centrales e implementación en la legislación española", *Redur*, Núm. 10, 2012, pp. 79-82

medida informal de la guarda de hecho. En cuanto a las primeras, son las establecidas por la persona con discapacidad, en las que designa quién debe prestarle apoyo y con qué alcance. Cualquier medida de apoyo voluntaria podrá ir acompañada de las salvaguardas necesarias para garantizar en todo momento y ante cualquier circunstancia el respeto a la voluntad, deseos y preferencias de la persona. Respecto a las segundas, procederán en defecto de la voluntad de la persona con discapacidad, esto es, solo cuando la persona con discapacidad no pueda o no haya expresado y diseñado su apoyo, lo hará la autoridad judicial. La guarda de hecho tiene un carácter subsidiario, dado que se aplica en defecto de no se introducirá si existen otras medidas voluntarias o judiciales que se estén aplicando eficazmente.

3.4.2. Las medidas de apoyo voluntarias:

Bajo el título "de las medidas voluntarias de apoyo", en el capítulo II del título XI del libro primero del Código Civil, entre los artículos 254 y 262, se regulan las medidas de apoyo que se establecen por voluntad de la propia persona con discapacidad. Procurando respetar los principios de la Convención, la reforma prioriza los instrumentos voluntarios sobre los establecidos judicialmente, evitando en lo posible que las medidas de apoyo las diseñe un tercero[245]. Dentro de las medidas voluntarias adquieren especial importancia los poderes y mandatos preventivos y la autocuratela.

Cualquier persona mayor de edad o menor emancipada en previsión o apreciación de la concurrencia de circunstancias que puedan dificultarle el ejercicio de su capacidad jurídica en igualdad de condiciones con las demás, podrá prever o acordar en escritura pública las medidas de apoyo relativas a su persona o bienes que precise para el adecuado ejercicio de su capacidad jurídica. Se trata de la posibilidad de delimitar libremente el sistema de apoyos de los que se ha de valer la persona para tomas decisiones, pudiendo delimitar tanto el régimen de su actuación, el alcance de las facultades de la persona o personas que le hayan de prestar apoyo, forma de ejercicio del apoyo, las medidas u órganos de control que estime oportuno, las salvaguardas necesarias para evitar abusos, conflicto de intereses o influencia indebida y los mecanismos, incluidos plazos de revisión de las medidas de apoyo, con el fin de garantizar el respeto de su voluntad, deseos y preferencias[246].

Cuando el artículo 255 CC menciona la idea de actuar "en previsión o apreciación", se refiere a las circunstancias actuales o futuras que dificulten o dificultarán la capacidad jurídica de la persona. Gracias a la introducción de esta apreciación se posibilita, por ejemplo, que una persona que ha sido diagnosticada de una enfermedad degenerativa o de un Alzheimer en estado inicial, pueda crear voluntariamente su medida de apoyo personal para el futuro. Este diseño voluntario de la medida debe realizarse mediante

[245] PEREÑA VICENTE, M., "Una contribución a la interpretación del régimen jurídico de las medidas de apoyo ene l ejercicio de la capacidad jurídica consagradas en la Ley 8/2021 de 2 de junio", en PEREÑA VICENTE, M., *El ejercicio de la capacidad jurídica por las personas con discapacidad tras la Ley 8/2021 de 2 de junio*, Tirant lo blanch, Valencia, 2022, p.172

[246] CERMI., "El impacto de la reforma del derecho civil", cit., p. 4

escritura pública, y será el notario quien, habiendo escuchado a la persona, la informe legalmente sobre la transcendencia de la medida. El notario autorizante comunicará de oficio y sin dilación el documento público que contenga las medidas de apoyo al Registro Civil para su constancia en el registro individual del otorgante. Esta obligación de comunicación del notario se introduce con el objetivo de que, ante un procedimiento para la constitución de un sistema de apoyo, se tenga conocimiento de la voluntad de la persona, y se actué en consecuencia. Ante la insuficiencia o deficiencia del documento que nace de la voluntad del sujeto, y a falta de la guarda de hecho, se introducirán medidas judiciales.

El notario debe asegurarse que la persona que crea su propia medida de apoyo lo realiza libremente y en base a su voluntad. Este debe asumir una labor que favorezca el adecuado desarrollo de las personas con discapacidad, promoviendo, como consagra la Convención, su inclusión en la sociedad, que en la medida posible su voluntad tenga cauce adecuado para regir su persona y bienes[247]. Para garantizar que las personas comprenderán el proceso que realizarán ante el notario, se podrán utilizar los apoyos, instrumentos y ajustes razonables que resulten precisos, incluyendo sistemas aumentativos y alternativos, braille, lectura fácil, pictogramas, dispositivos multimedia de fácil acceso, intérpretes, sistemas de apoyos a la comunicación oral, lengua de signos, lenguaje dactilológico, sistemas de comunicación táctil y otros dispositivos que permitan la comunicación, así como cualquier otro que resulte preciso[248].

Tras el paso por la notaria, el Registro Civil se convierte en una pieza central de articulación del sistema de apoyos, pues hará efectiva la preferencia que el nuevo sistema atribuye a las medidas voluntarias. No obstante, el respeto a los derechos fundamentales de la persona con discapacidad, incluida su intimidad y la protección de sus datos personales, han llevado a considerar que las medidas de apoyo accedan al Registro como datos sometidos al régimen de publicidad restringida[249].

El dato de la discapacidad aporta información relevante sobre el estado de salud de la persona a la que se refiere, por ello, el RGPD incluye expresamente a la discapacidad entre el listado de los datos relativos a la salud. Al identificarse la discapacidad como dato relativo a la salud, directamente se sitúa entre las categorías especiales de datos, las cuales, como viene reiterándose, merecen especial protección por ser particularmente sensibles en relación con los derechos y las libertades fundamentales[250]. En este mismo sentido, con anterioridad a la entrada en vigor del RGPD, en el Informe de 8 de julio de 2014 de la AEPD[251], se indicaba que la discapacidad es un dato especialmente

[247] UNIÓN INTERNACIONAL DEL NOTARIADO. Guía notarial de buenas prácticas para personas con discapacidad: El notario como apoyo institucional y autoridad pública, 2019, p. 41
[248] Artículo 25 de la Ley de Notariado de 28 de mayo de 1862, actualizado tras la Ley 8/2021
[249] En la nueva redacción del artículo 83 de la Ley 20/2011, de 21 de julio, del Registro Civil se introducen la discapacidad y las medidas de apoyo en la lista de los datos con publicidad restringida.
[250] Considerando 51 del RGPD
[251] AEPD. Informe jurídico núm. 178/2014 de 8 de julio de 2014

protegido, sin distinción del tipo de discapacidad, el carácter de especialmente protegido no depende del tipo de discapacidad, sino de la mera existencia de la misma[252].

Debido a este carácter especial, solo la persona inscrita o sus representantes legales (en caso de menores), quien ejerza el apoyo y que esté expresamente autorizado, el apoderado preventivo general o el curador podrán acceder o autorizar a terceras personas la publicidad de los asientos que contengan datos especialmente protegidos como los presentes. Las Administraciones Públicas y los funcionarios públicos podrán acceder a dichos datos cuando en el ejercicio de sus funciones deban verificar la existencia o el contenido de las medidas de apoyo. En el caso de que la persona inscrita fallezca, el Juez de Primera Instancia del domicilio del solicitante será el encargado de autorizar el acceso a los datos especialmente protegidos, siempre que justifique interés legítimo y razón fundada para pedirlo. Se presume que ostentan dicho interés legítimo el cónyuge del fallecido, la pareja de hecho y los ascendientes y descendientes hasta el segundo grado[253].

Finalmente, como crítica a las medidas voluntarias, se ha indicado que a diferencia de la persona con discapacidad que se encuentre en un entorno respetuoso en el que no exista riesgo de abuso podrá diseñar su medida de apoyo según su voluntad, el riesgo de abuso en las personas con discapacidad que se encuentran en entornos no respetuosos podrá verse incrementado[254]. Así, con la reforma se incrementa el riesgo de que intervenga una persona con intereses espurios, al margen o en contra de las previsiones adoptadas preventivamente, y en un caso extremo, llegue a forzar un cambio de parecer en la persona que prestará el apoyo que favorezca intereses espurios[255].

a) Los poderes y mandatos preventivos:

Regulados en los artículos 256-262 CC, los poderes y mandatos preventivos son declaraciones de voluntad que despliegan todos sus efectos como un negocio jurídico, debiendo acreditar el hecho que los motiva[256]. El principio del respeto a la autonomía de la voluntad de los mayores que sufren alguna dolencia progresiva, exige que deba atenderse prioritariamente a la voluntad del sujeto cuando éste haya expresado sus

[252] En el mismo sentido se pronuncia la AEPD en sus informe jurídicos núm. 2/2022 y núm. 80/2021 de de 29 de marzo de 2022 ambos

[253] Artículo 84 de la Ley del Registro Civil

[254] EQUIPO GIMÉNEZ SALINAS., "Principales novedades de la Ley 8/2021 por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad y Derecho Ley 19/2021 en Cataluña", *gimenez-salinas.es,* 26 de octubre de 2021, disponible en: https://gimenez-salinas.es/novedades-ley-8-2021-apoyo-personas-discapacidad/ *[Última consulta:205 de junio de 2022]*

[255] CABANAS TREJO, R., "Observaciones irrespetuosas sobre la Ley 8/2021 para la práctica notarial", *notariosyregistradores,* 8 de septiembre de 2021, disponible en: https://www.notariosyregistradores.com/web/secciones/oficina-notarial/otros-temas/observaciones-irrespetuosas-sobre-la-ley-8-2021-para-la-practica-notarial/ *[Última consulta: 20 de junio de 2022]*

[256] ESCARTÍN IPIÉNS, J.A., "La autocuratela en el Anteproyecto de Ley sobre modificación del Código Civil y otras leyes complementarias en materia de discapacidad»", *Revista de Derecho Civil*, Vol. 5, Núm. 3, 2018, p. 88.

deseos en cuanto al diseño de su futura asistencia[257]. Otorgar un poder es verificar una delegación de confianza en el apoderado**,** puesto que se le faculta para ejecutar determinadas acciones las cuales vincularán jurídicamente al que dio ese poder. El contenido del poder puede ser variadísimo, porque es la persona que lo otorga quien lo determina a su voluntad[258], es esta última quien determina quién, cuándo, en qué ámbito, para qué y cómo ejercerá este apoyo.

En consecuencia, las medidas referidas pueden ser relativas a la persona o a los bienes, así como, por ejemplo, relativas a la salud o cuidados médicos. Debe indicarse como adecuado el criterio seguido por el legislador de no introducir ninguna directriz sobre el contenido que deben tener, optando por fomentar la autonomía de la persona. Cuando se haya otorgado el poder a favor del cónyuge o de la pareja de hecho del poderdante, el cese de la convivencia producirá su extinción automática, salvo que esta extinción sea contraria a la voluntad del poderdante o que el cese de convivencia se produzca por su internamiento. A su vez, podrá establecer las medidas u órganos de control que estime oportuno, condiciones e instrucciones para el ejercicio de las facultades, salvaguardas para evitar abusos, conflicto de intereses o influencia indebida y los mecanismos y plazos de revisión de las medidas de apoyo, con el fin de garantizar el respeto de su voluntad, deseos y preferencias. Podrá también prever formas específicas de extinción del poder[259]. Aunque la ley no diferencia de manera expresa los tipos de poderes preventivos se podría distinguir entre los poderes preventivos para el futuro y los poderes preventivos que contienen una cláusula de subsistencia.

En cuanto a los primeros, que se ajustan a la definición tradicional de los poderes preventivos, son aquellos que se constituyen para un futuro en el que exista una discapacidad que requiera un apoyo específico. En base al artículo 257 CC, el poderdante podrá otorgar poder solo para el supuesto de que en el futuro precise apoyo en el ejercicio de su capacidad. Para acreditar que se ha producido la situación de necesidad de apoyo, se estará a las previsiones del poderdante. Para garantizar el cumplimiento de estas previsiones se otorgará, si fuera preciso, acta notarial que, además del juicio del notario, incorpore un informe pericial en el mismo sentido.

Respecto a los segundos, las cláusulas de subsistencia comienzan a producir efectos desde su otorgamiento, y subsistirán aun cuando el otorgante necesite apoyos para ejercer su capacidad jurídica. En otras palabras, se otorgan y comienzan a producir efectos, y el hecho de que se produzca una situación de discapacidad que requiera apoyos no tiene ningún efecto adverso en el poder.

Cuando el poder contenga cláusula de subsistencia para el caso de que el poderdante precise apoyo en el ejercicio de su capacidad o se conceda solo para ese supuesto y, el

[257] NÚÑEZ ZORRILLA, M.C., *La asistencia: la medida de protección de la persona con discapacidad psíquica alternativa al procedimiento judicial de incapacitación*, Dykinson, Madrid, 2014, p. 156
[258] GOMÁ LANZÓN, F., "Los poderes preventivos en la ley de apoyo a las personas con discapacidad", *Hay Derecho*, 8 de junio de 2021, disponible en: https://www.hayderecho.com/2021/06/08/los-poderes-preventivos-en-la-ley-de-apoyo-a-las-personas-con-discapacidad/ *[Última consulta: 20 de junio de 2022]*
[259] Artículo 258 CC

poder recoja todos los negocios del otorgante, sobrevenida la situación de necesidad de apoyo, el apoderado quedará sujeto a las reglas aplicables a la curatela en todo aquello que no se hubiese previsto en el poder, salvo que el poderdante haya determinado otra cosa[260].

Uno de los principales problemas que plantea este tipo de instrumentos radica en determinar el momento exacto en que concurre la necesidad de apoyo que pone en marcha el poder o mantiene la vigencia del poder que contenga la cláusula de subsistencia. El artículo 257 del CC deja al criterio del poderdante la inclusión de previsiones al respecto, y para garantizar el cumplimiento de estas previsiones se otorgará, si fuera preciso, acta notarial que, además del juicio del Notario, incorpore un informe pericial en el mismo sentido[261].

Tal y como se ha adelantado, los poderes preventivos, como medidas voluntarias, deben ser siempre notariales e inscribirse en el registro civil para que quede constancia de la voluntad del poderdante. Así, DE AMUNÁTEGUI RODRÍGUEZ[262] considera la inscripción en el Registro Civil un presupuesto de seguridad jurídica, puesto que, se respeta la voluntad de la persona, evitando que existan apoderamientos en manos de otros, en cuyo caso pueda ignorarse y ocultarse su presencia a la hora de adoptar una medida de apoyo judicial, rompiendo con todas las premisas y principios de la Convención.

Los poderes mantendrán su vigencia pese a la constitución de otras medidas de apoyo a favor del poderdante, tanto si estas han sido establecidas judicialmente como si han sido previstas por el propio interesado. El poder preventivo, es ilimitado en el tiempo, si bien el poderdante puede establecer cautelas para su revisión y extinción. Mediante la introducción de mecanismos y plazos de revisión de las medidas de apoyo, se pretende garantizar el respeto de su voluntad, deseos y preferencias[263]. Cuando concurra alguna de las causas previstas para la remoción del curador en el apoderado[264], cualquier persona legitimada para instar el procedimiento de provisión de apoyos y el curador[265], si los hubiere, podrán solicitar judicialmente la extinción de los poderes preventivos.

Según indica la nueva redacción del artículo 1732 del CC, los mandatos se extinguirán por la revocación, la renuncia del mandatario, la muerte o por concurso del mandante o del mandatario, el establecimiento en relación al mandatario de medidas de apoyo que

[260] Artículo 259 CC
[261] LÓPEZ AZCONA, A., "Medidas voluntarias de apoyo", en CERDEIRA BRAVO DE MANSILLA, G.; GARCÍA MAYO, M.; GIL MEMBRADO, C. y PRETEL SERRANO, J.J., *Un nuevo orden jurídico para las personas con discapacidad*, Wolters Kluwer, Madrid, 2021, p. 372
[262] DE AMUNÁTEGUI RODRÍGUEZ, C., "El protagonismo de la personas con discapacidad en el diseño y gestión del sistema de apoyo", *cit*., p. 150
[263] FERNÁNDEZ TRESGUERRES, A., *El ejercicio de la capacidad jurídica: comentario práctico de la ley 8/2021, de 2 de junio*, Aranzadi, Pamplona, 2021, p. 105
[264] En este sentido dice el artículo 278 CC que *"Serán removidos de la curatela los que, después del nombramiento, incurran en una causa legal de inhabilidad, o se conduzcan mal en su desempeño por incumplimiento de los deberes propios del cargo, por notoria ineptitud de su ejercicio o cuando, en su caso, surgieran problemas de convivencia graves y continuados con la persona a la que prestan apoyo".*
[265] Artículo 258 CC y 51bis de la Ley 15/2015 de jurisdicción voluntaria

incidan en el acto en que deba intervenir en esa condición; o la constitución en favor del mandante de la curatela representativa como medida de apoyo para el ejercicio de su capacidad jurídica, a salvo lo dispuesto en este Código respecto de los mandatos preventivos.

b) Autocuratela:

Regulada en los artículos 271-274 del CC, se puede definir como una manifestación de voluntad, en virtud de la cual el potencial beneficiario, una persona física, mayor de edad, menor emancipado o habilitado de edad en previsión de que se produzca una eventual y futura situación de discapacidad que requiera apoyo continuado, propone la curatela como medida de apoyo necesaria para el adecuado ejercicio de su capacidad jurídica, desarrollo de su personalidad y condiciones de igualdad. A su vez, se trata de una situación jurídica de salvaguarda o medida institucional de apoyo, puesto que, tal declaración de voluntad vincula a la autoridad jurídica y genera una situación jurídica de conformidad con la extensión y límites de la resolución judicial que constituya la curatela, regulada por las disposiciones del declarante, por lo declarado en la resolución judicial y lo establecido por la ley[266]. La declaración de voluntad vincula a la autoridad judicial generando una situación jurídica, y su extensión y límites se fijan en la resolución judicial que constituya la curatela[267]. La meritada posibilidad legal, no es otra cosa que el reconocimiento de la dignidad de la persona, que comprende la facultad de autodeterminarse; o, dicho de otro modo, de ser protagonista de su propia existencia, de adoptar las decisiones más transcendentes, que marcan su curso vital, según sus deseos y preferencias, en la medida en que quepa satisfacerlos[268].

Se trata de un negocio jurídico *inter vivos* que se inscribe dentro del derecho de familia, de carácter unilateral, pues proviene de la voluntad del otorgante sin necesidad de concordarla con la propia de la persona designada al tiempo de su otorgamiento y desencadena sus efectos en vida de la persona con discapacidad. Es personalísimo, pues pertenece exclusivamente a la esfera dispositiva de la persona que la ejerce en tanto en cuanto le compete la designación de la persona que, en virtud de su disponibilidad, solicitud, empatía, cercanía y afecto, considera más idónea para prestarle los apoyos precisos para el ejercicio de su capacidad jurídica en condiciones de igualdad, para acompañarla, asistirla o incluso excepcionalmente representarla, con la confianza que ejercerá dicho cargo con respeto a su voluntad, deseos, preferencias, creencias, valores y trayectoria vital. Por otra parte, es solemne, puesto que su validez precisa que la voluntad se manifieste en escritura pública notarial, como las medidas voluntarias de apoyo, y vincula al juez al proceder al nombramiento de curador, sin perjuicio de que

[266] LÓPEZ SAN LUIS, R., "El principio de respeto a la voluntad de la persona con discapacidad en la Convención de Nueva York y su reflejo en el anteproyecto por la que se reforma la legislación civil y procesal en materia de discapacidad", *InDret*, Núm. 2, 2020, pp.130-131

[267] ESCARTÍN IPIÉNS, J.A., "La autocuratela en el Anteproyecto de Ley sobre modificación del Código Civil y otras leyes complementarias en materia de discapacidad", *cit.*, p. 87

[268] STS Sala de lo Civil 465/2019, de 17 de septiembre de 2019 (Rec. Núm. 5199/2018)

pueda prescindir de dicha designación mediante resolución motivada, por razones graves, desconocidas al tiempo del otorgamiento o por alteración de las circunstancias tenidas en cuenta en el momento de la designación. Las facultades de la persona no solo se limitan a la designación de quien vaya a ejercer las funciones de curador, incluso sus sustitutos, sino también contempla la opción de establecer las disposiciones que se consideren oportunas con respecto al funcionamiento y ejercicio del cargo[269].

A diferencia de las medidas voluntarias que pueden ser también de presente, la autocuratela se refiere a una situación de dificultad en el ejercicio de la capacidad jurídica del futuro, y así lo remarca el artículo 271 del CC "*en previsión de la concurrencia de circunstancias que puedan dificultarle el ejercicio de su capacidad jurídica en igualdad de condiciones con las demás, podrá proponer en escritura pública el nombramiento o la exclusión de una o varias personas determinadas para el ejercicio de la función de curador*". El presupuesto es que aún no se ha dado esa situación de dificultad en el ejercicio de su capacidad jurídica[270].

La autocuratela se parece a la figura de la autotutela[271] del régimen anterior, puesto que, la autotutela se definía como la facultad de una persona con capacidad de obrar suficiente para designar en documento público notarial a su futuro tutor. Esta institución, eliminada por la reforma, no existió hasta la entrada en vigor de la Ley 41/2003, de 18 de diciembre, de Protección Patrimonial de las personas con discapacidad y de modificación del Código Civil, de la Ley de enjuiciamiento Civil y de la normativa tributaria con esta finalidad, y fue adoptada del Código de Familia Catalán[272] como la facultad de designación del propio tutor u otras medidas de disposición relativas a la propia persona o bienes del incapaz[273] atribuida a cualquier persona con capacidad de obrar suficiente en previsión de ser incapacitado judicialmente en el futuro[274]. Aunque la autotutela sea el origen de la autocuratela, ha de remarcarse que en esta nueva figura no hay cabida para los conceptos de "tutor", "capacidad de obrar suficiente" e "incapacitado judicialmente". Por ello, se podría decir que se trata de la antigua autotutela adecuada al marco de la CDPD.

---

[269] STS Sala de lo Civil 734/2021, de 2 de noviembre de 2021 (Rec. Núm. 1201/2021)

[270] DE SALAS MURILLO, S., "De la autocuratela", en GUILARTE MARTÍN-CALERO, C. (dir)., *Comentarios a la ley 8/2021 por la que se reforma la legislación civil y procesal en materia de* discapacidad, Aranzadi, Pamplona, 2021, p. 703

[271] Fue el Abogado del Estado Sánchez Torres quien introdujo el término de la "autotutela", aunque el que recomendó la introducción de esta figura fue Crehuet del Amo, que la denominó "tutela fiduciaria" definiéndola como la guarda de la persona y bienes deferida por mandato o comisión del sujeto a ella, antes de haber incidido en incapacidad. Por tanto, se trata de la designación de tutor hecha por un individuo en plena capacidad jurídica para el caso en que deje de ser capaz. Véase al respecto: BELLO JANEIRO, D., "Una mirada crítica sobre la regulación de la autotutela" en PÉREZ VARGAS MUÑOZ, J., *Congreso Internacional de Derecho Civil. La encrucijada de la incapacitación y la discapacidad*, La Ley. Madrid, 2011, pp. 372-373

[272] Artículo 172 de la Ley 9/1998, de 15 de julio, del Código de Familia

[273] Véase en este aspecto: SERRANO GARCÍA, I., *Autotutela: el artículo 223-ii, del código civil y la convención de nueva york, sobre derechos de las personas con discapacidad de 2006, cit.*, pp. 101-105

[274] GONZÁLEZ GRANDA, P., *Régimen jurídico de protección de la discapacidad por enfermedad mental, cit.*, p. 112

En base al artículo 271 del CC, la declaración voluntad debe realizarse en escritura pública donde se nombrará o excluirá a una o varias personas[275] determinadas para ejercer el cargo de curador. Podrá igualmente establecer disposiciones sobre el funcionamiento y contenido de la curatela y, en especial, sobre el cuidado de su persona, reglas de administración y disposición de sus bienes, retribución del curador, obligación de hacer inventario o su dispensa y medidas de vigilancia y control, así como proponer a las personas que hayan de llevarlas a cabo. Al igual que ocurría con la autotutela[276], no es preciso que el interesado mencione las razones que le impulsan a proponer a determinadas personas, ni tampoco las que le impulsan a excluirlas.

Esta declaración es vinculante para la autoridad judicial, salvo que mediante resolución motivada exprese que existen circunstancias graves desconocidas por la persona que las estableció que desaconsejen ese nombramiento[277]. La competencia de la autoridad judicial es a su vez recogida en el artículo 275.1 del CC, donde se recoge que serán curadores las personas que "a juicio de la autoridad judicial" sean aptas para el adecuado desempeño de su función. En definitiva, se da prioridad a la voluntad del sujeto[278] excepto cuando la autoridad judicial entienda que existen causas que disuaden tal nombramiento. La diferencia entre el poder preventivo y la autocuratela radica en el control judicial que se aplica en la última. Así, aunque la declaración de voluntad vincule inicialmente a la autoridad judicial, este tiene la facultad de prescindir de las medidas adoptadas por el disponente mediante resolución motivada[279]. Esta posibilidad de prescindir total o parcialmente de la disposición voluntaria tiene una función protectora, puesto que la sustitución de la voluntad se realiza cuando se prevea una actuación inadecuada por parte del curador por la existencia de circunstancias graves desconocidas por la persona en el momento de realizar la declaración.

Es de interés referir en este punto la sentencia del Tribunal Supremo de 19 de octubre de 2021[280], la cual resolvió que no había ninguna razón que avalase prescindir de la voluntad de la persona con discapacidad. El caso trataba sobre una mujer que padecía un deterioro cognitivo leve-moderado por demencia senil y síndrome depresivo, quien había otorgado testamento abierto, en el cual, en su cláusula cuarta, constaba su voluntad de nombrar a su hija como tutora (con los respectivos sustitutos) en caso de que fuera necesario, y que en ningún caso se nombrará tutor a cualquiera de los otros tres hijos ni a ninguna asociación, ni pública ni privada ni a ningún organismo similar. Esta voluntad no fue respetada por considerar que la hija, con quien además convivía, era inidónea para el ejercicio de tal función, y se constituyó una tutela mancomunada atribuida a los dos hijos varones, de los cuales uno de ellos estaba expresamente excluido por la madre. El Tribunal Supremo expresó que era cierto que el Código Civil permite alterar o incluso prescindir de todas las personas designadas, pero bajo un doble

[275] El artículo 277 del CC permite, en caso de que sea necesario, nombrar a más de un curador.
[276] DURÁN CORSANEGRO, E., *La autorregulación de la tutela*, Ramón Areces, Madrid, 2007, p. 138
[277] STS Sala de lo Civil 298/2017, de 16 de mayo de 2017 (Rec. Núm. 298/2017)
[278] STS Sala de lo Civil 487/2014, de 30 de septiembre de 2014 (Rec. Núm. 18/2014)
[279] STS Sala de lo Civil 458/2018, de 18 de julio de 2018 (Rec. Núm. 4374/2017)
[280] STS Sala de lo Civil 706/2021, de 19 de octubre de 2021 (Rec. Núm. 305/2021)

condicionamiento: que concurran circunstancias que así lo justifiquen, pues la regla general es respetar el orden preestablecido, y que tales razones resulten debidamente explicitadas en la resolución judicial que así lo acuerde, con una motivación suficiente.

La resolución recurrida no exteriorizaba las razones que necesariamente debían concurrir para prescindir de la persona designada en primer lugar para el ejercicio del cargo de tutora (actualmente curadora), con la que convivía desde hace años y asumía de facto el papel de cuidadora principal, sin que bastase al respecto la mera remisión, sin valoración crítica alguna, al informe elaborado por los servicios psicosociales que daban una simple opinión, lo cual debía ser apreciada críticamente. El Alto Tribunal indicaba que, aún en el caso de considerar que la hija no reunía las condiciones necesarias para ejercer la asignada función, se debía respetar el orden preestablecido, cosa que no se hico, nuevamente sin fundamentación jurídica. Por ello, concluyó que la argumentación de la sentencia recurrida era pobre, insuficiente y desligada de las circunstancias del proceso. En consecuencia, declaró que el recurso debía ser estimado, puesto que no se respetó la voluntad de la demandada, sin razones que avalasen una decisión de tal clase, pues no concurrían los requisitos para prescindir dicha voluntad.

3.4.3. Las medidas de apoyo legales o judiciales:

Se ha dicho ya que las medidas de apoyo legales o judiciales solo serán adoptadas en defecto o insuficiencia de la voluntad de la persona con discapacidad. Estas medidas de apoyo han estar inspiradas en el respeto a la dignidad de la persona y en la tutela de sus derechos fundamentales, y deben ajustarse a los principios de necesidad y proporcionalidad. Dentro de las medidas legales o judiciales, también denominadas como formales, se identifican dos tipos: la curatela, que se aplica a quienes precisan el apoyo de modo continuado, y el defensor judicial, cuando la necesidad de apoyo se precisa de forma ocasional, aunque sea recurrente.

Todas las medidas de apoyo adoptadas judicialmente serán revisadas periódicamente en un plazo máximo de tres años o, en casos excepcionales, en un plazo máximo de seis años. En todo caso, pueden ser revisadas ante cualquier cambio en la situación de la persona que pueda requerir su modificación. Este control es un ejemplo de la flexibilidad que ha pretendido otorgar el legislador al sistema de apoyo ya que, alejándose del antiguo sistema estático de sustitución, en caso de que cambie la situación de la persona, este apoyo podrá ser adaptado a la nueva circunstancia.

En cuanto a la retribución por el apoyo otorgado, el artículo 281 del CC indica que el curador tiene derecho a una retribución, siempre que el patrimonio de la persona con discapacidad lo permita, así como al reembolso de los gastos justificados y a la indemnización de los daños sufridos sin culpa por su parte en el ejercicio de su función, cantidades que serán satisfechas con cargo a dicho patrimonio. La autoridad judicial es la encargada de fijar su importe y el modo de percibirlo, para lo cual tendrá en cuenta el trabajo a realizar y el valor y la rentabilidad de los bienes. La Ley otorga un tratamiento distinto en las diferentes partidas: si se trata de la retribución será a cargo del patrimonio

del apoyado siempre que cuente con patrimonio para ello, lo cual permite pensar que esa retribución podría satisfacerse por otras vías: patrimonio de familiares, asociaciones o fundaciones o, incluso, prestaciones de la seguridad social. En cambio, el reembolso de los gastos y la indemnización de daños siempre se imputa al patrimonio de la persona que precisa el apoyo[281].

Si bien la normativa regula la retribución por el apoyo otorgado del curador, no hace lo mismo en el caso del defensor judicial. Entre los artículos 295 y 298 CC responsables de la regulación de la figura del defensor judicial de la persona con discapacidad, se realizan ciertas remisiones a la normativa del curador (causas de inhabilidad, excusa, remoción…). Sin embargo, para los demás supuestos no contemplados como el presente, se encuentra un vacío legal. En base a la aplicación analógica de las normas, se entiende que lo procedente será recurrir a la normativa de curatela. En consecuencia, se reconoce la posibilidad de solicitar una indemnización por daños y perjuicios sufridos sin su culpa y que se deriven del ejercicio de la medida[282].

a) Curatela:

El curador viene a ser una especie de báculo o compañero de camino que no toma decisiones "en lugar de" la persona sino "con" ella. La autonomía de la persona debe limitarse lo menos posible[283], lo que requiere un exhaustivo conocimiento judicial de sus concretas circunstancias vitales, tras el cual ha de confeccionarse el traje a medida[284] (no *"prêt-à-porter"*, sino personalizado y exclusivo para ella)[285]. En este sentido, la sentencia del Tribunal Supremo de 19 de febrero de 2020 consideró que la curatela es una medida proporcional que respeta la autonomía e independencia individual, sin menoscabo de la protección de sus intereses[286].

---

[281] MUNAR BERNAT, P., "A. La curatela: Principal medida de apoyo de origen judicial para las personas con discapacidad", *Revista de Derecho civil*, Vol. 5, Núm. 3, 2018, pp. 140-141

[282] DÍAZ PARDO, G., "Retribución y gastos derivados del ejercicio de la medida de apoyo a la persona con discapacidad. Nuevas perspectivas tras la Ley 8/2021, de 2 de junio, de reforma de la legislación civil y procesal", *Revista de Derecho Civil*, Vol. 9, Núm. 1, 2022, p. 107

[283] En este sentido, en la sentenica de 15 de mayo de 2018 el Tribunal Supremo admitió que la tutela establecida mediante la sentencia recurrida era desproporcional, ya que aunque el demandado necesitara ayuda para algunas cosas, mantenía plenas facultades de discernimiento y decisión sobre cuestiones de la vida ordinaria, y administraba perfectamente su patrimonio. De ahí que, partiendo del principio de plena capacidad de las personas, fuese necesario un apoyo para el tratamiento médico prescrito, lo cual era acorde con el nombramiento de curador. STS Sala de lo Civil 362/2018, de 15 de mayo 2018 (Rec. Núm. 2122/2017).

[284] La STS Sala de lo Civil 552/2017, de 11 de octubre de 2017 (Rec. Núm. 2065/2016), aún siendo previa a la reforma, habla de medidas de apoyo en vez del sistema de sustitución, y recalca la idea del traje a medida. Asimismo, considera a la incapacitación total como una medida desmesurada, y mantiene el régimen de curatela por tratarse del medio de apoyo adecuado.

[285] VIVAS TESÓN, I., "La reforma civil y procesal para el apoyo de las personas con discapacidad: ¿A partir de septiembre, qué?", *hayderecho*, 13 de junio de 2021, disponible en: https://www.hayderecho.com/2021/06/13/la-reforma-civil-y-procesal-para-el-apoyo-de-las-personas-con-discapacidad-a-partir-de-septiembre-que/ *[Última consulta: 22 de junio de 2022]*

[286] STS Sala de lo Civil 118/2020, de 19 de febrero de 2020 (Rec. Núm. 3904/2019)

El preámbulo de la Ley entiende que la curatela es la principal medida de apoyo de origen judicial para las personas con discapacidad, por tratarse de una figura graduable a las circunstancias y necesidades de la persona con discapacidad. Como se ha adelantado, la etimología de la palabra curatela (cuidado) revela la finalidad de la institución: asistencia, apoyo, ayuda en el ejercicio de la capacidad jurídica. Esta medida formal de apoyo se aplica a quienes precisen el apoyo de modo continuado, y su extensión viene determinada en la correspondiente resolución judicial en armonía con la situación y circunstancias de la persona con discapacidad[287]. Aun tratándose de la principal medida de origen judicial, es preciso tener en cuenta que su existencia solo puede justificarse ante la inexistencia o insuficiencia de otra medida[288].

La sentencia del Tribunal Supremo de 16 de mayo de 2017[289] alega que la curatela es una institución flexible que se caracteriza por su contenido de asistencia y supervisión, no por el ámbito personal o patrimonial o por la extensión de actos en los que esté llamada a prestarse. Indica que este apoyo puede utilizarse tanto en el ámbito personal como en el patrimonial, su uso no está limitado a un único ámbito, el curador puede llevar a cabo apoyo tanto en la esfera personal como patrimonial[290]. En el mismo sentido se pronuncia la sentencia del Tribunal Supremo de 27 de septiembre de 2017[291], relativa a una mujer con síndrome de Down sometida a una incapacitación total, situación que "es inadecuada y excesiva" siendo más idóneo la intervención del curador, tanto en la esfera personal como en la patrimonial que la apoye en los actos que recoge la sentencia.

Se distinguen dos distintos tipos de curatela: la curatela asistencial y la curatela representativa. La primera se refiere a una curatela "normal", en la cual el curador otorga un apoyo a la persona en el ejercicio de su capacidad jurídica teniendo siempre en cuenta sus preferencias, voluntades y deseos. En cuanto a la segunda, solo aplicable ante una situación de discapacidad grave que impida a la persona decidir por sí misma, el curador representa a la persona, pero su actuación deberá respetar igualmente las preferencias, voluntades y deseos de su representado. Como principio de actuación y en la línea de excluir en lo posible las actuaciones de naturaleza representativa, la curatela será, primordialmente, de naturaleza asistencial. No obstante, en los casos en los que sea preciso, y solo de manera excepcional, podrá atribuirse al curador funciones

[287] La STS Sala de lo Civil 341/2014, de 1 de julio de 2014 (Rec. Núm. 1365/2012), indica que la curatela se concibe en términos más flexibles, puesto que será la sentencia quien expresamente imponga en qué actos asistirá el curador. En el mismo sentido: STS Sala de lo Civil 124/2018, de 7 de marzo de 2018 (Rec. Núm. 4192/2016) y STS Sala de lo Civil 244/2015, de 13 de mayo de 2015 (Rec. Núm. 846/2014)
[288] Artículo 269 del CC
[289] STS Sala de lo Civil 298/2017 de 16 de mayo de 2017 (Rec. Núm. 2759/2016). En el mismo sentido: STS Sala de lo Civil 421/2013 de 24 de junio de 2013 (Rec. Núm. 1220/2012), STS Sala de lo Civil 553/2015 de 14 de octubre de 2015 (Rec. Núm. 1257/2014), STS Sala de lo Civil 557/2015 de 20 de octubre de 2015 (Rec. Núm. 2158/2014), STS Sala de lo Civil 373/2016 de 3 de junio de 2016 (Rec. Núm. 2367/2015), STS Sala de lo Civil 216/2017 de 4 de abril de 2017 (Rec. Núm. 56/2016), STS Sala de lo Civil 118/2018 de 6 de marzo de 2018 (Rec. Núm. 1632/2017), STS Sala de lo Civil 458/2018 de 18 de julio de 2018 (Rec. Núm. 4374/2017) y STS Sala de lo Civil 269/2021 de 6 de mayo de 2021 (Rec. Núm. 2235/2020)
[290] STS Sala de lo Civil 124/2018, de 7 de marzo de 2018 (Rec. Núm. 4192/2016)
[291] STS Sala de lo Civil 530/2017, de 27 de septiembre de 2017 (Rec. Núm. 183/2017)

representativas. Todas las personas, y en especial las personas con discapacidad, requieren ser tratadas por las demás personas y por los poderes públicos con cuidado, es decir, con la atención que requiera su situación concreta.

Como critica, puede alegarse que, en los casos más extremos, la curatela representativa terminará siendo equivalente a la tutela. Esto es, aunque la figura sustitutiva ha sido eliminada por la reforma, cuando la discapacidad sea muy elevada (por ejemplo un estado vegetativo en el que se encuentre la persona), el curador terminará tomando todas las decisiones en nombre de la persona con discapacidad. No obstante, aún en una situación tan extrema, el curador deberá actuar respetando la voluntad, los deseos y las preferencias de la persona.

La constitución de la medida corresponde a la autoridad judicial, quien la adoptará mediante resolución motivada y determinará los actos para los que la persona requiere asistencia del curador en el ejercicio de su capacidad jurídica atendiendo a sus concretas necesidades de apoyo. Los actos en los que el curador deba prestar el apoyo deberán fijarse de manera precisa, indicando, en su caso, cuáles son aquellos donde debe ejercer la representación. Para nombrar al curador, la autoridad judicial podrá optar una persona mayor de edad que considere apta o elegir una fundación u otra persona jurídica sin ánimo de lucro, pública o privada, entre cuyos fines figure la promoción de la autonomía y la asistencia[292].

Desde la perspectiva negativa se distingue entre quienes no pueden ser curadores y quienes no podrán ser designados judicialmente como tales, salvo circunstancias extraordinarias, motivadas en la resolución judicial. Las primeras se refieren a las excluidas preventivamente por la persona, por resolución judicial de la patria potestad o total o parcialmente de los derechos de guardia y custodia o los removidos de una tutela, curatela o guardia legal. Las restantes causas susceptibles de excepción se relacionan con el conflicto de interés y la mala gestión económica[293]. Una vez haya tomado posesión de su cargo ante el letrado de la Administración de Justicia, comenzará a asistir a la persona en el ejercicio de su capacidad jurídica respetando su voluntad, deseos y preferencias, y siempre tratará de que la persona con discapacidad pueda desarrollar su propio proceso de toma de decisiones.

En el caso del curador con facultades representativas, este estará obligado a hacer un inventario del patrimonio de la persona en cuyo favor se ha establecido el apoyo ante el letrado de la Administración de Justicia dentro del plazo de sesenta días, a contar desde aquel en que hubiese tomado posesión de su cargo[294]. En base al artículo 287 del CC, el curador que ejerza funciones de representación necesitará autorización judicial para los actos que determine la resolución.

[292] Artículo 275 del CC
[293] FERNÁNDEZ TRESGUERRES, A., *El ejercicio de la capacidad jurídica: comentario práctico de la ley 8/2021, de 2 de junio, cit.*, pp. 125-126
[294] Artículos 282 y 285 del CC

El curador puede ser removido de su cargo cuando incurra en una causa legal de inhabilidad, desempeñe mal el cargo, por notoria ineptitud de su ejercicio o cuando, en su caso, surgieran problemas de convivencia graves y continuados con la persona a la que presta apoyo. La autoridad judicial, de oficio o a solicitud de la persona a cuyo favor se estableció el apoyo o del Ministerio Fiscal podrá decretar la remoción del curador mediante expediente de jurisdicción voluntaria. Durante la tramitación del expediente de remoción la autoridad judicial podrá suspender al curador en sus funciones y, de considerarlo necesario, acordará el nombramiento de un defensor judicial. Una vez declarada judicialmente la remoción, se procederá al nombramiento de un nuevo curador, salvo que fuera pertinente otra medida de apoyo[295]. El cargo se extinguirá por la muerte o declaración de fallecimiento de la persona con medidas de apoyo, por resolución judicial cuando ya no sea precisa esta medida de apoyo o cuando se adopte una forma de apoyo más adecuada para la persona sometida a curatela[296].

b) Defensor judicial:

La actualizada figura del defensor judicial como medida formal de apoyo se regula entre los artículos 295 y 298 del CC[297], y procede cuando la necesidad de apoyo se precisa de forma ocasional, aunque sea recurrente, de ahí que se configure como una medida judicial de apoyo no estable.

Se identifican distintos escenarios para que entre en juego la presente medida. El primer supuesto se refiere al caso en el que la persona que haya de prestar el apoyo no pueda hacerlo. Aquí se pueden identificar dos situaciones: una transitoria que imposibilite por un periodo de tiempo limitado prestar el apoyo, y una definitiva que imposibilite totalmente dicha actividad. Ante esta última situación, se nombrará al defensor judicial mientras se nombre a otra persona para ocupar el cargo. El segundo escenario alude a un conflicto de intereses entre la persona con discapacidad y la que haya de prestarle apoyo[298], ante esta situación de conflicto, procederá nombrar al defensor judicial para que apoye a la persona que lo necesite.

Respecto al tercer caso, se nombrará a un defensor judicial cuando el curador haya alegado una excusa para no ejercer el cargo y la autoridad judicial lo considere necesario hasta resolver acerca de la excusa alegada. Será excusable el desempeño de la curatela si resulta excesivamente gravoso o entraña grave dificultad para la persona nombrada para el ejercicio del cargo. También podrá excusarse el curador de continuar ejerciendo la curatela cuando durante su desempeño le sobrevengan los motivos de excusa. Las personas jurídicas privadas podrán excusarse cuando carezcan de medios

[295] Artículo 278 del CC
[296] Artículo 291 del CC
[297] Previa a la reforma se regulaba entre los artículos 299-302 del CC
[298] La sentencia del Tribunal Supremo de 17 de enero de 2003 recoge que el conflicto de intereses existe cuando, al realizar los actos de guarda y protección, la actuación de los representantes pone en peligro el beneficio del menor o de la persona con discapacidad, por tratarse de un acto contrario al interés de este. STS Sala de lo Civil 212/2003, de 17 de enero 2003 (Rec. Núm. 2083/1997).

suficientes para el adecuado desempeño de la curatela o las condiciones de ejercicio de la curatela no sean acordes con sus fines estatutarios. Se establece un plazo de quince días desde que se tenga conocimiento del nombramiento para poder alegar la causa de excusa, si la causa fuera sobrevenida se podrá hacerlo en cualquier momento[299].

El cuarto escenario se refiere al caso en el que se haya promovido la provisión de medidas judiciales de apoyo a la persona con discapacidad y la autoridad judicial considere necesario proveer a la administración de los bienes hasta que recaiga resolución judicial. En este caso, mientras se finalice el procedimiento de provisión de medidas judiciales de apoyo, se podrá nombrar a un defensor judicial en caso de que sea necesario. Por último, se nombrará a un defensor judicial cuando la persona con discapacidad requiera el establecimiento de medidas de apoyo de carácter ocasional, aunque sea recurrente.

Tal y como indica el artículo 296 del CC, en el caso de que se haya encomendado el apoyo a más de una persona, no se nombrará al defensor judicial, salvo que ninguna pueda actuar o la autoridad judicial motivadamente considere necesario el nombramiento, por ello, la presente figura tiene un carácter subsidiario ante los apoyos múltiples. A su vez, a esta figura le son aplicables las mismas causas de inhabilidad, excusa y remoción del curador. Igualmente, el defensor judicial tendrá la obligación de conocer y respetar la voluntad, deseos y preferencias de la persona a la que deba prestar el apoyo[300]. La autoridad judicial deberá puntualizar las concretas funciones que le asigna o los asuntos en los que tendrá intervención, dependiendo del caso para que es designado. Como en el anterior sistema, los distintos supuestos y la medida de apoyo a la que se sustituya influirán en su ámbito de actuación. El marco general del defensor, como el de todas las medidas de apoyo, consistirá en asistir a la persona con discapacidad en el ejercicio de su capacidad jurídica en los ámbitos en los que sea preciso, respetando en todo momento su voluntad, deseos y preferencias[301].

3.4.4. Guarda de hecho:

El preámbulo de la Ley objeto de análisis indica que, dentro de las medidas voluntarias adquieren especial importancia los poderes y mandatos preventivos, así como la posibilidad de la autocuratela, y que fuera de ellas destaca el reforzamiento de la figura de la guarda de hecho. Con la introducción de la frase "fuera de ellas", se subraya que la guarda de hecho no será bajo ningún concepto una medida de apoyo voluntaria. A su vez, como se ha adelantado, el artículo 250 del CC indica que las medidas de apoyo para el ejercicio de la capacidad jurídica de las personas que lo precisen son, además de las de naturaleza voluntaria, la guarda de hecho, la curatela y el defensor judicial.

[299] Artículo 279 del CC
[300] Artículo 297 del CC
[301] ÁLVAREZ LATA, N., "Del defensor judicial de la persona con discapacidad", en BERCOVITZ RODRÍGUEZ-CANO, R.(Coord.)., *Comentarios al Código Civil*, Aranzadi, Pamplona, 2021, pp. 535-536

Tras la reforma, se identifica como una medida informal de apoyo para las personas con discapacidad[302], y se regula entre los artículos 263 y 267 del CC. Se ha convertido en una auténtica institución jurídica de apoyo, al dejar de ser una situación provisional cuando se manifiesta como suficiente y adecuada para la salvaguarda de los derechos de la persona con discapacidad. Por regla general, se entiende que la persona con discapacidad está bien apoyada en la toma de decisiones y en el ejercicio de su capacidad jurídica por un guardador de hecho que generalmente es un familiar[303], pues la familia sigue siendo en nuestra sociedad el grupo básico de solidaridad y apoyo entre las personas que la componen. Por ello, el guardador de hecho será alguna persona del entorno y confianza de la persona con discapacidad, constituyendo una relación informal pero no carente de relevancia jurídica[304].

Esta medida de apoyo que no requiere un nombramiento, ni voluntario ni judicial, nace de la práctica diaria en la que, cuando una persona requiere un apoyo para el ejercicio de su capacidad jurídica, es asistida por alguna persona de su círculo cercano como puede ser un familiar. Lo que tiene de peculiar la guarda de hecho es que surge *ex facto*, pero una vez surgida es una institución jurídica; o, lo que es lo mismo, es una institución jurídica *ex post facto*[305]. El hecho de que no requiera ningún nombramiento hace que esta figura sea identificada como informal. Asimismo, el artículo 263 del CC indica que la persona que venga ejerciendo adecuadamente la guarda de hecho de una persona con discapacidad continuará en el desempeño de su función incluso si existen medidas de apoyo de naturaleza voluntaria o judicial, siempre que estas no se estén aplicando eficazmente. Es decir, la guarda de hecho no es incompatible con las medidas voluntarias o judiciales, sino con el funcionamiento eficaz de dichas medidas. Por ello, se deduce que tiene un lugar secundario entre las medidas de apoyo, puesto que no se introducirá si existen otras medidas voluntarias o judiciales que se estén aplicando eficazmente.

La guarda surge desde el momento en que una persona, física o jurídica, sin tener asignadas facultades tutelares, se encarga voluntariamente de apoyar a otra con respecto a la cual no le une ningún tipo de obligación derivada de una previa sentencia de incapacitación. Se trata de la asunción de obligaciones voluntarias por la persona que decide asistir a una persona que requiere el apoyo[306]. En relación directa con los principios de necesidad y proporcionalidad de las medidas de apoyo, la guarda de hecho solo existe si es necesaria para el ejercicio de la capacidad jurídica de la persona con discapacidad. No obstante, si existe y se manifiesta como suficiente y adecuada para la

[302] Se separan expresamente la guarda de hecho del menor (artículos 237 y 238 del CC) y la guarda de hecho de las personas con discapacidad (artículos 263-267 del CC)
[303] ZURITA MARTÍN, I., "La esperada y necesaria reforma del Código Civil en materia de personas con discapacidad", *Revista de Estudios Jurídicos y Criminológicos*, Núm. 3, 2021, p. 14
[304] ROMERO COLOMA, A.M., *Capacidad, incapacidad e incapacitación*, *cit.*, p. 98
[305] PAU, A., "El principio de igualdad y el principio de cuidado, con especial atención a la discapacidad", *Revista de Derecho Civil*, Vol. 7, Núm. 1, 2020, p. 11
[306] MONJE BALMACEDA, O., "El estado de la cuestión: La guarda de hecho. Instrumento clave en las instituciones de apoyo", en LLEDÓ YAGÜE, F.; MONJE BALMACEDA, O. y GUTIERREZ BARRENENGOA, A., *Estudio básico sobre la guarda de hecho: algunas reflexiones sustantivas y procesales notables de lege data y de lege ferenda*, Dykinson, Madrid, 2019, p. 59

persona con discapacidad, resulta una medida normal, estable y con vocación de permanencia, independientemente de la gravedad de la situación de la persona o de la intensidad que exijan las medidas de apoyo. La guarda de hecho, en su configuración actual y con los refuerzos de la nueva regulación, se puede adaptar perfectamente a cualquier situación[307]. De esta forma la guarda de hecho tendrá un papel esencial para facilitar a las personas con discapacidad el ejercicio de sus derechos[308].

El ámbito ordinario de su actuación se circunscribe a los actos de carácter personal y de cuidado y asistencia necesarios y, tratándose de actos de carácter patrimonial, se incluyen los actos de administración ordinaria del patrimonio de la persona guardada. El guardador de hecho, por definición, no está investido de un cargo, por lo que carece de legitimación para actuar en el tráfico jurídico en representación de la persona[309]. Esto es, el guardador de hecho no tiene funciones representativas de la persona con discapacidad, por ello, cuando ante un caso excepcional, se requiera la actuación representativa del guardador de hecho, este deberá de obtener la autorización a través del correspondiente expediente de jurisdicción voluntaria en el que se oirá a la persona con discapacidad. Tras comprobar la necesidad de la representación y con los requisitos adecuados a las circunstancias del caso, se otorgará la autorización judicial para actuar como representante. Esta autorización podrá comprender uno o varios actos necesarios para el desarrollo de la función de apoyo y deberá ser ejercitada de conformidad con la voluntad, deseos y preferencias de la persona con discapacidad[310].

En todo caso, y al igual que ocurre en la curatela representativa, quien ejerza la guarda de hecho deberá recabar autorización judicial para, entre otras cuestiones, realizar actos de transcendencia personal o familiar cuando la persona con discapacidad no pueda hacerlo por sí misma. En el ámbito sanitario, el artículo 9.3.a) de la LBAP recoge la actuación representativa del guardador de hecho para otorgar el consentimiento informado al introducir el precepto "las personas vinculadas a el por razones familiares o de hecho"[311].

Los supuestos de extinción de la guarda de hecho[312] pueden consistir en que la persona a quien se preste apoyo solicite que este se organice de otro modo. Este punto subraya nuevamente la idea de la reforma de respetar en todo momento la voluntad, deseos y preferencias de la persona con discapacidad, puesto que se permite que la guardad de hecho se extinga por la voluntad de esta. El segundo supuesto se refiere a la desaparición de las causas que motivaron la medida de la guarda de hecho, tanto si la persona no necesita más ese apoyo o si cobran eficacia las medidas de apoyo dispuestas

[307] ÁLVAREZ LATA, N., "Del defensor judicial de la persona con discapacidad", *cit.*, p. 493
[308] FERRÉ, E.A., "La nueva guarda de hecho como verdadera institución de apoyo", *Revista Boliviana de Derecho*, Núm. 30, 2020, p. 172
[309] PEREÑA VICENTE, M., "La transformación de la guarda de hecho en el Anteproyecto de Ley", *Revista de Derecho Civil*, Vol. 5, Núm. 3, 2018, p. 76
[310] Artículo 264 del CC
[311] En este sentido: PARRA LUCÁN, M.A., "La guarda de hecho de las personas con discapacidad", en DE SALAS MURILLO, S. (Coord.)., *Los mecanismos de guarda legal de las personas con discapacidad tras la convención de naciones unidas*, Dykinson, Madrid, 2013, p. 255
[312] SALAZAR VARELLA, C.E., *El proceso de incapacitación*, *cit.*, p. 349

que no funcionaban. El tercer escenario alude al desistimiento del guardador de hecho, acto que deberá realizarse de manera expresa indicando su voluntad de no seguir siendo el guardador de hecho de la persona con discapacidad. Por último, la figura de la guarda de hecho será extinguida cuando lo solicite el Ministerio Fiscal o quien pretenda ejercer dicha función y la autoridad judicial la acuerde.

4. LA NECESIDAD DE UNA NUEVA INTERPRETACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES TRAS LA REFORMA:

Tal y como se indicaba en la introducción del presente capítulo, tras el examen realizado de la Ley 8/2021, una de las principales cuestiones que ha de ser estudiada es el efecto que el nuevo sistema de apoyos produce en la capacidad de las personas mayores con discapacidad a la hora de otorgar el consentimiento para el tratamiento de sus datos relativos a la salud. El "consentimiento del interesado", concepto que será analizado en profundidad en el siguiente capítulo, es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado, como titular de sus datos personales, acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de los mismos[313]. Este consentimiento cobra ciertos matices en el caso de las personas mayores, puesto que entran en juego conceptos como la brecha digital entre otros, pero, en el caso de las personas mayores con discapacidad, esta condición añade una capa más de vulnerabilidad, de ahí que se deba analizar específicamente el otorgamiento de este consentimiento del interesado cuando es ejercido por una persona mayor con discapacidad.

La aplicación de las nuevas tecnologías de información y comunicación en el ámbito sanitario pretende mejorar la calidad de vida de las personas mayores, fomentando un envejecimiento activo y saludable. No obstante, cabe preguntarse si las personas mayores, y más concretamente, las personas mayores con discapacidad, son las que verdaderamente autorizan el tratamiento de sus datos relativos a la salud que realizan estas nuevas tecnologías; y en el mismo sentido, si se pueden tratar los datos relativos a la salud de las mismas al margen de su voluntad, o si pueden estar monitorizadas en contra de su voluntad en base a su interés superior. A su vez, aunque los interesados tengan determinados derechos como titulares de los datos, el ejercicio de los mismos por parte de las personas mayores con discapacidad plantea ciertas interrogantes que han de ser resueltas.

Por todo lo antedicho, en los siguientes capítulos se realizará una nueva lectura de la normativa de protección de datos de conformidad con la Ley 8/2021, con el fin de responder a las preguntas identificadas en la introducción general del presente trabajo. Específicamente, en el capítulo tercero se analizará si las personas mayores con discapacidad pueden otorgar el consentimiento del interesado para el tratamiento de sus datos relativos a la salud. En el capítulo cuarto se estudiará si pueden otorgar el

[313] Artículo 4.11 del RGPD

consentimiento del interesado para autorizar el tratamiento de sus datos relativos a la salud en el ámbito específico de la investigación en salud. Por último, en el capítulo quinto se analizará si pueden ejercer personalmente los derechos que recoge la normativa de protección de datos personales, y si tienen la posibilidad indicar en un documento cuál es su voluntad en cuanto al tratamiento de sus datos relativos a la salud que pueda realizarse tras su muerte.

CAPÍTULO 3: EL CONSENTIMIENTO DEL INTERESADO COMO BASE LEGITIMADORA PARA EL TRATAMIENTO DE LOS DATOS RELATIVOS A LA SALUD EN ENTORNOS CONECTADOS

1. INTRODUCCIÓN:

Desde su incepción, el consentimiento del interesado ha constituido el núcleo del sistema europeo de protección de datos. Aunque pueda verse como una base legitimadora más, lo cierto es que, hasta la fecha, las normas declaran que el consentimiento del interesado constituye la principal herramienta que legitima el tratamiento de los datos personales, y más concretamente de los datos relativos a la salud, objeto del presente estudio. Mediante el mismo, se ha querido asegurar que sea la persona, desde su libertad individual, la que decida cómo, cuándo y para qué se tratarán sus datos personales. En este sentido, es importante recordar que el consentimiento del interesado fue ideado para proporcionar a cada persona un control sobre su información personal.

Con todo, el valor del consentimiento como instrumento de control, y de protección del interesado, ha sido criticado debido a que el desarrollo tecnológico que se ha producido en los últimos años ha banalizado el valor de dicho consentimiento a través de formas más blandas que llevan a prestarlo casi por defecto. Por ello, en los tiempos en los cuales la obtención y el análisis masivo de datos es una práctica habitual, cabe preguntarse si realmente el consentimiento sigue siendo una herramienta adecuada para proteger el derecho a la protección de datos personales del sujeto en un mundo dominado por las TIC o por el contrario debemos considerarla una herramienta obsoleta que es preciso sustituir o al menos complementar.

Dado que el primer capítulo ha sido motivado por la necesidad de exponer el estado de la cuestión en materia de ventajas y riesgos tecnológicos, y el segundo capítulo ha estado enfocado al análisis de la nueva realidad jurídica que crea la reforma operada por la Ley 8/2021, en este capítulo nos centraremos en analizar la normativa de protección de datos personales. En este capítulo, tras una contextualización breve del derecho que nos ocupa, procuraremos en primer lugar identificar los diversos tipos de datos que existen con el fin de comprender la naturaleza de cada uno de ellos y así diferenciarlos de los datos relativos a la salud que constituyen la base de este trabajo. Seguidamente, se estudiarán los requisitos del consentimiento del interesado para comprender la causa de esta base legitimadora para el tratamiento de los datos personales. Dada la importancia que el RGPD ha otorgado al derecho a la información y al principio de transparencia con el fin de reforzar el consentimiento del interesado, estos derechos serán analizados de un modo separado al resto en el cuarto epígrafe.

Tras analizar los fundamentos de este derecho, la siguiente labor será dilucidar si el reforzamiento de los requisitos del consentimiento por parte de la normativa vigente ha sido suficiente, o si se han de fomentar las herramientas técnicas de protección

colectiva, a saber, la protección de datos desde el diseño y por defecto que se recoge en el artículo 25 del RGPD, y la certificación como elemento que acredita el cumplimiento del citado artículo, alejándonos de la solución del sistema individualista del consentimiento del interesado.

Por último, se examinará la necesidad de incorporar la reforma de la discapacidad en la interpretación del consentimiento del interesado mayor con discapacidad para el tratamiento de los datos relativos a su salud. Es nuestra intención que este enfoque del consentimiento permita comprender de forma íntegra y aportar novedad a la nueva realidad proyectada por la Ley 8/2021 en el ámbito de protección de datos. Pero, el análisis del concepto del consentimiento de las personas mayores discapacitadas no se agota en este capítulo, ya que en el siguiente, referente a la investigación en salud, se analizará la posibilidad que tienen las personas mayores con discapacidad de otorgar consentimiento para el tratamiento de los datos personales con fines de investigación en salud tras la entrada en vigor de la referida Ley 8/2021.

2. EVOLUCIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS COMO FACULTAD DE CONTROL DE LOS DATOS PERSONALES:

Como es sabido, el derecho a la protección de datos personales es resultado de un largo e intenso recorrido a partir de la segunda mitad del siglo XIX[314]. El Convenio 108 del Consejo de Europa fue el primer instrumento internacional jurídicamente vinculante adoptado en el ámbito de la protección de datos. Dicho Convenio surgió para desarrollar la protección de los derechos fundamentales de las personas en relación con el uso de la informática, y fijar las bases para una legislación internacional que permitiera compatibilizar el flujo internacional de datos[315]. En su primera formulación, el objetivo de este nuevo derecho a la protección de datos personales consiste en garantizar a

[314] Tradicionalmente, los derechos humanos han sido categorizados en tres generaciones. Esta categorización fue inicialmente propuesta en 1979 por el jurista VAŠÁK en el Instituto Internacional de Derechos Humanos, y su división pretendía seguir las nociones centrales de las tres frases que fueron la base de la revolución francesa: Libertad, Igualdad y Fraternidad. En la primera generación se encuentran los derechos civiles y políticos, considerados como derechos de defensa de las libertades del individuo. Imponen al Estado el deber de abstenerse de interferir en el ejercicio y pleno goce de estos derechos por parte del ser humano. La segunda generación, corresponde a los derechos económicos, sociales y culturales, que requieren una política activa de los poderes públicos encaminada a garantizar su ejercicio, es decir, requieren una acción positiva del estado. En la tercera generación, se encuentran los llamados derechos solidarios, incluyéndose en ella derechos heterogéneos como el derecho a la paz, a la calidad de vida o las garantías frente a la manipulación genética. Sin embargo, el desarrollo de la informática y de las nuevas tecnologías dio lugar al nacimiento de la cuarta generación de derechos humanos, en la cual se encuentra el derecho a la protección de datos. Las tres generaciones de derecho humanos no eran suficientes para hacer frente a la nueva realidad que supuso la revolución tecnológica, y como consecuencia se tuvo que crear una cuarta generación de derechos humanos relacionados directamente a las nuevas tecnologías y a la incidencia estas en la vida de las personas. En este sentido, cualquier avance tecnológico plantea nuevos retos para la normativa de protección de datos. Véase al respecto: DOMARADZKI, S.; KHVOSTOVA, M. y PUPOVAC, D., "Karel Vasak's Generations of Rights and the Contemporary Human Rights Discourse. Human Rights Review", Vol. 20, Núm. 4, 2019, pp. 424-426; ÁLVAREZ CARO, M., *Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la era digital*, Reus, Madrid, 2015, p. 58

[315] ÁLVAREZ HERNANDO, J., *Practicum protección de datos,* Aranzadi, Pamplona, 2018, pp. 48-49

cualquier persona física el respeto de sus derechos y libertades fundamentales, concretamente a su vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona.

En España, el presente derecho tiene sus cimientos en el artículo 18.4 de la Constitución Española[316]. La Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Automatizado de los Datos de Carácter Personal[317], conocida como LORTAD, fue la primera ley en materia de protección de datos a nivel estatal. Por su parte, en el año 1995, se aprobó la Directiva 95/46/CE del Parlamento y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos[318]. En estado español, en el año 1999, entró en vigor la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD). Un año más tarde, en el marco de la Unión Europea, la carta de los Derechos Fundamentales[319], recogió en su artículo 8 la protección de datos de carácter personal. Según la formulación recogida en este instrumento de carácter constitucional, toda persona tiene derecho a la protección de los datos de carácter personal que la conciernan. Además, establece que estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Actualmente, las normas jurídicas en vigor en España en materia de protección de datos son el RGPD por el que se deroga la Directiva 95/46/CE, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD) por la que se deroga la LOPD.

El derecho a la protección de datos personales fue definido por el Tribunal Constitucional, en su Sentencia 292/2000 de 30 de noviembre de 2000, como el derecho de las personas a disponer sus datos personales. Tal y como afirma la sentencia, el derecho fundamental a la protección de datos persigue garantizar a las personas un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado. Esta garantía impone a los poderes públicos la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías, junto con el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información.

La jurisprudencia del TC ha puesto de manifiesto en sucesivas sentencias que el objeto de protección del derecho fundamental a la protección de datos no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales. Por consiguiente, también alcanza a aquellos datos personales que pese a ser accesibles al conocimiento de cualquiera no escapan al poder de disposición del afectado, porque así lo garantiza su derecho a la protección de datos. Asimismo, el que

[316] STC 96/2012 de 7 de mayo de 2012 (BOE núm. 134 de 5 de junio de 2012)
[317] BOE núm. 262, de 31 de octubre de 1992
[318] BOE núm. 298, de 14 de diciembre de 1999
[319] *DOUE núm. C 083 de 30 de marzo de 2010*

los datos sean de carácter personal no significa que solo tengan protección los relativos a la vida privada o íntima de la persona, sino que los datos amparados son todos aquellos que identifiquen o permitan la identificación de la persona, pudiendo servir para la confección de su perfil ideológico, racial, sexual, económico o de cualquier otra índole, o que sirvan para cualquier otra utilidad que en determinadas circunstancias constituya una amenaza para el individuo[320].

Por otra parte, el contenido del derecho fundamental a la protección de datos consiste, en un poder de disposición y control sobre los datos personales, tanto frente al Estado como ante cualquier particular[321]. Permite al individuo saber quién posee esos datos personales y para qué los quiere utilizar, pudiendo el interesado oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como sus posibles usos por parte de un tercero, sea el Estado o un particular[322].

En el año 2000, la importante sentencia del Tribunal Constitucional desvinculó el derecho a la protección de datos del derecho a la intimidad, configurándolo como un derecho fundamental independiente. Brevemente, cabe recordar que el derecho a la intimidad fue definido como el derecho a "ser dejado en paz"[323]. El derecho a la intimidad del artículo 18.1 de la Constitución tiene el objetivo de ofrecer una protección constitucional eficaz de la vida privada y familiar, atribuyendo a su titular un haz de facultades que consisten en el poder jurídico de imponer a terceros la realización u omisión de determinados comportamientos. Actualmente, el poder vedar o proteger parcelas de la vida de la persona física del conocimiento ajeno se ha convertido en una

[320] Fundamento jurídico 6 de la STC 292/2000 de 30 de Noviembre de 2000 (BOE núm. 4 de 4 de enero de 2000)

[321] FERNÁNDEZ LÓPEZ, J. M., "El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario", *Derecho y salud*, Vol. 11, Núm. 1, 2003, p. 40

[322] Fundamento jurídico 7 de la STC 292/2000 de 30 de Noviembre de 2000

[323] Fue en el año 1890 cuando los juristas norteamericanos Warren y Brandéis sentaron las bases técnico-jurídicas del derecho a la intimidad en su monografía "*The Rigt to Privacy*", el cual se traduce como "el derecho a la privacidad o intimidad". Los autores afirmaron que los nuevos inventos provocaron que se tomaran las medidas necesarias para proteger a las personas, creando el derecho de "ser dejado en paz" ("*to be let alone*"). Alegaban que las fotografías instantáneas y los periódicos, entre otros, habían invadido el espacio sagrado de la vida doméstica, haciendo que "lo susurrado en el armario fuese proclamado desde los techos de las casas". En el citado trabajo, se puso de relieve el delicado equilibrio entre el derecho a informar y ser informado y el derecho a la intimidad del individuo. La proliferación de avances tecnológicos amenazaba con la difusión indiscriminada de información privada, divulgándose los más íntimos detalles en las columnas de los periódicos para satisfacer la curiosidad lasciva mediante la intromisión en el ámbito privado. Frente a las posibilidades invasivas de la tecnología, manifestaban la necesidad de definir un principio que pudiese ser invocado para amparar la intimidad del individuo frente a la invasión de una prensa demasiado pujante, del fotógrafo, o del poseedor de cualquier otro moderno aparato de grabación o reproducción de imágenes o sonidos. Este principio, se materializaba en el derecho a la intimidad, que le otorgaba a toda persona plena disponibilidad para decidir en qué medida podían ser comunicados a otros sus pensamientos, sentimientos y emociones. Véase al respecto: WARREN, S.D. y BRANDEIS, L.D. "The right to privacy", *Harvard law review*, vol.4, no.5, 1890, p. 195; SALDAÑA, M.N., "The right to privacy: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis", *Revista de Derecho Político*, Núm. 85, 2012, pp.210-211

forma de ejercitar la libertad individual. Así, el bien jurídico último que representa esa se configura como es el derecho a la intimidad[324].

Este último tiene por objeto garantizar un ámbito reservado de su vida, vinculado con el respeto de su dignidad como persona, frente a la acción y el conocimiento de los demás, sean éstos poderes públicos o simples particulares. Atribuye a su titular el poder de resguardar ese ámbito reservado, no solo personal sino también familiar frente a la divulgación del mismo por terceros y una publicidad no querida. No garantiza una intimidad determinada sino el derecho a poseerla, disponiendo a este fin de un poder jurídico sobre la publicidad de la información relativa al círculo reservado de su persona y su familia, con independencia del contenido de aquello que se desea mantener al abrigo del conocimiento público[325]. Es decir, el derecho a la intimidad impide que se revelen aspectos de la vida privada y familiar que una persona ha querido reservar del conocimiento público[326].

Por su parte, de forma complementaria al planteamiento anterior, el derecho fundamental a la protección de datos persigue garantizar un poder de control sobre sus datos personales, sobre su uso y destino. Su objeto es diferente del derecho a la intimidad, ya que el derecho a la protección de datos personales amplía la garantía constitucional a aquellos datos que sean relevantes o que tengan incidencia en el ejercicio de cualesquiera derechos de las personas, sean o no constitucionales y sean o no relativos al honor, la ideología, la intimidad personal y familiar o a cualquier otro bien constitucionalmente amparado. Se configura así como un derecho fundamental autónomo e independiente del derecho a la intimidad[327], cuya finalidad, objeto y contenido difieren, habida cuenta de los distintos riesgos que ambos derechos fundamentales han de enfrentar en las sociedades actuales[328]. En consecuencia, se puede afirmar que el derecho a la protección de datos es un derecho de la personalidad por su condición de derecho inherente a la persona[329]. El bien jurídico tutelado es propio de la persona, y necesario para el pleno desarrollo de su personalidad, su vulneración priva a la persona del disfrute y goce de sus derechos y libertades[330].

---

[324] MURILLO DE LA CUEVA, P., "El derecho a la autodeterminación informativa y la protección de datos personales", *Azpilcueta*, Núm. 20, 2008, pp. 45-46

[325] STC 115/2000 de 5 de mayo (BOE núm. 136 de 7 de junio de 2000)

[326] SÁNCHEZ GONZÁLEZ, M.P., *Honor, intimidad y propia imagen*, Jurúa, Lisboa. 2017, p. 89

[327] La diferencia se encuentra en que el derecho a la intimidad impone a terceros un deber de no intromisión en la esfera íntima de las personas, pero el derecho a la protección de datos, además, le confiere al titular ciertas facultades consistentes en diversos poderes jurídicos cuyo ejercicio impone a terceros deberes jurídicos no recogidos en el derecho a la intimidad. El derecho a la protección de datos no constituye una manifestación más del derecho a la intimidad, sino que como instrumento jurídico de tutela de la dignidad y el libre desarrollo de la personalidad, alcanza en el ordenamiento jurídico sustantividad propia, configurándose como derecho a la personalidad. Véase al respecto: HERRÁN ORTIZ, A.I., "El derecho a la protección de datos personales en la sociedad de información", *Cuadernos Deusto de Derechos Humanos*, Núm. 26, 2003, p.21

[328] GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación ubicua*, Dykinson, Madrid, 2016, p. 96

[329] AEPD, Informe jurídico 365/2006 de 10 de agosto de 2006 y 0278/2009 de 3 de junio de 2009

[330] HERRÁN ORTIZ, A.I., "El derecho a la protección de datos personales en la sociedad de información", *cit.*, p.16

Se trata en definitiva de impedir la instrumentalización del ser humano, que debe poder interactuar en la sociedad digital con plena libertad, con las mismas garantías que en el mundo físico. No en vano, las personas demandan protección frente al abuso del tratamiento de sus datos personales por parte de los poderes públicos y también frente a la actuación de los particulares.

En cualquier caso, como cualquier derecho, también la protección de los datos es un derecho relativo y no absoluto[331]. Es sabido que todos los derechos fundamentales están sujetos a límites, y así lo declaró en relación al derecho fundamental que nos ocupa el Tribunal de Justicia de la Unión Europea en su Dictamen 1/15 de 26 julio de 2017, al afirmar que los derechos consagrados en los artículos 7 y 8 de la Carta no constituyen prerrogativas absolutas, sino que deben considerarse según su función en la sociedad[332]. Por otra parte, y como complemento de las instrucción exegéticas aplicables al derecho que nos ocupa, en el apartado 140 del citado Dictamen se recoge que la protección del derecho fundamental al respeto de la vida privada en el ámbito de la Unión exige, con arreglo a la jurisprudencia reiterada del Tribunal de Justicia, que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario.

3. DEFINICIÓN DE DATO PERSONAL Y TIPOLOGÍA DE DATOS EN FUNCIÓN DE SU NIVEL DE SENSIBILIDAD:

Como puede colegirse del análisis de las nuevas tecnologías que se ha realizado en el primer capítulo del presente trabajo, se han de diferenciar diversos tipos de datos personales vinculados a la salud conectada, a saber, datos personales, categorías especiales de datos personales, datos relativos a la salud, datos genéticos, datos biométricos y datos ambientales.

El dato personal se define en el artículo 4.1 del RGPD como toda información sobre una persona física identificada o identificable ("el interesado o el titular de los datos personales"). La expresión "toda información" indica la voluntad del legislador de otorgar un sentido amplio al concepto de datos personales, debiendo realizarse una interpretación amplia del mismo. Son ejemplos de datos personales, entre otros, el nombre y el apellido, el domicilio, el número de documento nacional de identidad, el correo electrónico, pero también los datos de localización, la dirección de protocolo de internet (IP) o el identificador de una *cookie*[333]. Dado el sentido amplio que se le ha querido otorgar al citado artículo, esta lista ha de ser comprendida como *numerus apertus*.

---

[331] Considerando 4 del RGPD: *"El derecho a la protección de los datos personales* ***no*** *es un derecho absoluto sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad."*

[332] TJUE (Gran Sala) Dictamen 1/15 de 26 julio 2017, ECLI:EU:C:2017:592, apartado 136.

[333] GT29. Dictamen 4/2007 sobre el concepto de datos personales, 01248/07/ES (WP 136), 20 de junio de 2007, p. 6

Un dato o conjunto de datos relacionados con una persona física se considera identificable cuando su identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre o una dirección de IP. Se puede considerar "identificada" a una persona física cuando dentro de un grupo de personas se la "distingue" de todos los demás miembros del grupo. Por consiguiente, la persona física es "identificable" siempre que exista la posibilidad de hacerlo[334]. Para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física.

Para medir esta posibilidad de identificación, se ha de atender a criterios "temporales" y de "esfuerzo". Esto es, se han de considerar todos los factores objetivos, como los costes y el tiempo necesarios para la identificación, teniendo en cuenta tanto la tecnología disponible en el momento del tratamiento como los avances tecnológicos. Si mediante los medios que puedan ser utilizados por el responsable del tratamiento o por cualquier otra persona no es posible identificar a la persona en un periodo de tiempo razonable, el dato no se considerará personal[335].

Los datos personales, cifrados o presentados con un seudónimo pero que puedan utilizarse para volver a identificar a una persona son datos personales, y se les aplica la normativa de protección de datos. Los datos personales que hayan sido anonimizados, de forma que la persona no sea identificable o deje de serlo, dejarán de considerarse datos personales y no se les aplicará la normativa de protección de datos. Para que los datos se consideren verdaderamente anónimos, la anonimización debe ser irreversible[336].

Dentro de los datos personales, no todos poseen la misma importancia, dado que no todos los datos referidos a una persona física inciden de igual forma en la esfera de su intimidad, por lo tanto, no son objeto del mismo nivel de protección. Merecen especial protección los datos personales que por su naturaleza son particularmente sensibles, ya que su tratamiento podría conllevar importantes riesgos para los derechos y las libertades fundamentales. A estos datos se les conoce como categorías especiales de datos personales. La protección reforzada que se otorga a las categorías especiales de datos personales se realiza mediante la prohibición de su tratamiento que se recoge en el artículo 9.1 del RGPD, aunque esta prohibición admite excepciones tal y como se expondrá en el presente trabajo[337].

Los datos relativos a la salud constituyen un tipo especial dentro de las categorías de datos personales, y se definen como datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que

[334] Ibid., p. 13
[335] Considerando 26 del RGPD
[336] COMISIÓN EUROPEA. "¿Qué son los datos personales?", disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es *[Última consulta: 17 de abril de 2021]*
[337] Artículo 9.2 del RGPD

revelen información sobre su estado de salud[338]. El concepto de "dato relativo a la salud" ha suscitado controversias en relación a su perímetro. En general hay acuerdo en que los datos relativos a la salud pueden ser equiparados a los conceptos de "datos sanitarios" o "datos médicos", los cuales son más restrictivos y no abarcan, entre otras cuestiones, la información del estado de salud física o mental de la persona física y la información que se deriva de su asistencia sanitaria. La Directiva de Protección de Datos optó por utilizar el término dato relativo a la salud, aunque no proporcionó ninguna definición del mismo creando inseguridad jurídica. El RGPD se sumó al mismo uso pero, a diferencia de la Directiva, introdujo una delimitación más detallada del mismo.

Siguiendo la normativa del RGPD, entre los datos personales relativos a la salud se incluyen todos los datos relativos al estado de salud del interesado que dan información sobre su estado de salud física o mental pasada, presente o futura. En esta definición se incluyen los siguientes aspectos: la información sobre la persona física recogida con ocasión de su inscripción a efectos de asistencia sanitaria, o con ocasión de la prestación de tal asistencia; todo número, símbolo, imagen o dato proveniente de una persona física que la identifique de manera unívoca a efectos sanitarios; la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro[339].

La decisión del RGPD de adoptar un concepto tan amplio como el que se ha descrito pretende que la normativa de protección de datos logre abarcar la realidad que puedan crear los futuros avances tecnológicos. En cuanto a la LOPDGDD, la Disposición Adicional Decimoséptima regula el "tratamiento de datos de salud" a nivel nacional, aunque la misma disposición se base en el artículo 9 del RGPD. En este trabajo, se prefiere el término de "datos relativos a la salud" por entender que se trata de un concepto más adecuado a la realidad actual.

Junto con los datos relativos a la salud, es necesario mencionar a los datos genéticos[340], aunque se traten de dos diversas categorías de datos[341]. El artículo 4.13 del RGPD los define como datos personales relativos a las características genéticas heredadas o

[338] Artículo 4.15 del RGPD
[339] Considerando 35 del RGPD
[340] En este sentido, la AEPD afirmó que "*si bien es posible que del resultado del análisis de ADN no codificante no se deriven directamente datos de salud, dichos resultados vienen a conformar la huella genética de una persona, y por tanto, se encuentran íntimamente relacionados con su salud"*. Véase al respecto: AEPD. Memoria 2000, p. 171, disponible en: https://www.aepd.es/es/documento/memoria-aepd-2000.pdf
[341] GUILLÉN CATALÁN, R., "Sujetos responsables por vulneración de las normas de protección de datos. Especial referencia a los datos relativos a la salud", *Revista Boliviana de Derecho,* Núm. 30, 2020, p. 49

adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente[342]. Por su parte, siguiendo la línea del artículo 2.i) de la Declaración Internacional de la UNESCO sobre los Datos Genéticos Humanos, el artículo 3.j) de la Ley 14/2007, sobre Investigación Biomédica define los datos genéticos como información sobre las características hereditarias de una persona, identificada o identificable obtenida por análisis de ácidos nucleicos u otros análisis científicos. Aunque ha existido un debate sobre la posible configuración de los datos genéticos como datos relativos a la salud[343], este fue superado mediante el RGPD, el cual los separó como dos tipos diversos de datos pero los sigue manteniendo a ambos dentro de las categorías especiales de datos personales[344].

Entre las categorías especiales de datos se encuentran igualmente los datos biométricos, que constituyen datos personales relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos[345]. La biometría es un método de reconocimiento de personas basado en sus características físicas, fisiológicas o de comportamiento; un proceso similar al que habitualmente realiza el ser humano reconociendo e identificando a las personas por su aspecto físico, su voz, su forma de andar etc. La tecnología ha permitido automatizar y perfeccionar estos procesos de reconocimiento biométrico[346], por ejemplo, hoy en día, se pueden desbloquear los teléfonos inteligentes con las huellas dactilares o mediante el reconocimiento facial. Al igual que con los datos relativos a la salud, la normativa de protección de datos otorga a los datos biométricos una protección especial, y su tratamiento está prohibido, aunque existen excepciones. Dentro de los datos biométricos, se distinguen dos grupos: datos biométricos físicos y fisiológicos, y datos biométricos de comportamiento[347].

Como ejemplos de los datos biométricos físicos o fisiológicos podemos citar los siguientes: la huella dactilar, una de las más utilizadas debido a que se considera que las huellas dactilares son únicas e inalterables; el reconocimiento facial, es una técnica que utiliza programas de cálculo que analizan imágenes de rostros humanos para reconocer a una persona a partir de una imagen o fotografía; el reconocimiento de iris, el cual

[342] Considerando 34 del RGPD
[343] VILLARES, D.J., "Datos relativos a la salud y datos genéticos: consecuencias jurídicas de su conceptualización". *Revista Derecho y Salud Universidad Blas Pascal*, Núm. 1, Vol. 1, 2017, p. 62
[344] El GT29 también apostó por diferenciar los relativos conceptos al indicar que "los datos genéticos revelan características inherentes que los singularizan, en particular si se comparan con los datos de salud". Véase al respecto: GT29. Documento de Trabajo sobre Datos Genéticos, 12178/03/ES (WP 91), 17 de marzo de 2004, p. 4
[345] Artículo 4.14 del RGPD
[346] INCIBE. Tecnología biométricas aplicadas a la ciberseguridad: una guía de aproximicación para el empresario, *cit.*, p. 4
[347] INCIBE. Tecnología biométricas aplicadas a la ciberseguridad: una guía de aproximicación para el empresario, *cit.*, pp. 5-12

utiliza las características del iris humano con el fin de verificar la identidad de un individuo; el reconocimiento de la geometría de la mano, esta tecnología utiliza la forma de la mano para confirmar la identidad del individuo empleando una serie de cámaras que toman imágenes en 3D de la mano desde diferentes ángulos; el reconocimiento de la retina, se basa en la utilización del patrón de los vasos sanguíneos contenidos en la misma, puesto que cada patrón es único (incluso en gemelos idénticos al ser independiente de factores genético); y el reconocimiento vascular, extrae el patrón biométrico a partir de la geometría del árbol de venas del dedo o de las muñecas.

En el segundo grupo se encuentran, por ejemplo, el reconocimiento de voz, se utilizan aplicaciones con algoritmos que miden las muestras para identificar a las personas y el reconocimiento de escritura de teclado, se mide la fuerza de tecleo, la duración de la pulsación y el periodo de tiempo que pasa entre que se presiona una tecla y otra, el patrón de escritura en teclado que es permanente y propio de cada individuo.

Por último, se hace referencia a los datos ambientales, entre los cuales se encuentran, entre otros, la luz, la temperatura, la humedad o los niveles de CO2 de una habitación. A diferencia de los tipos de datos analizados anteriormente, los datos ambientales no se encuentran regulados específicamente en la normativa de protección de datos. Sin embargo, se trata de datos personales porque pueden dar información sobre las costumbres de las personas. Valga como ejemplo el uso de los aplicativos domóticos que controlan los horarios de uso de la luz o de la calefacción, lo cual permite saber si esa persona vive sola o acompañada y los horarios en los que se encuentra en casa. Por todo ello, pueden ser clasificados como datos personales, dado que otorgan una información social determinada de una persona. En este mismo sentido, el Tribunal Supremo declaró que los datos de consumo energéticos domésticos son datos personales por reflejar determinados hábitos de conducta privados de una persona física identificable, lo cual atañe sustancialmente a la esfera privada de la intimidad de cada consumidor[348]. En el ámbito sanitario, los datos ambientales son captados por dispositivos que permiten, por ejemplo, adaptar las características ambientales de las habitaciones de los hospitales en base a las necesidades del paciente.

4. EL CONSENTIMIENTO DEL INTERESADO O AFECTADO PARA EL TRATAMIENTO DE LOS DATOS RELATIVOS A LA SALUD:

4.1. Sobre el concepto del consentimiento del interesado o afectado:

En el ámbito del derecho a la protección de datos, el consentimiento constituye una de las bases legitimadoras para el tratamiento de datos personales[349], erigiéndose como una

[348] STS, Sala Tercera, de lo Contencioso-administrativo, sección 3ª, núm.1062/2019 de 12 de julio de 2019 (Rec. Núm. 4980/2018)

[349] El artículo 6 del RGPD recoge las bases legitimatorias para el tratamiento de los datos personales, dentro de las cuales se encuentra el consentimiento del interesado. A su vez, el artículo 9.2 del RGPD recoge las bases legitimatorias para el tratamiento de categorías especiales de datos personales. En este

forma de autorización autónoma. El concepto de "autorización autónoma" se refiere a que el interesado otorga un permiso por sí mismo, sin depender de nadie, para que se proceda al tratamiento de sus datos personales. Es decir, el titular de los datos autoriza al responsable del tratamiento para que este los procese. El "acto transformador" que el consentimiento produce consiste en que, lo que de otro modo se consideraría una violación del derecho a la protección de datos del individuo no es percibido como tal.

Al hablar de consentimiento, tanto el RGPD como la LOPDGDD hablan de "manifestación de voluntad", y es exactamente así como ha de ser catalogado dicho acto jurídico. Una manifestación de voluntad que produce efectos jurídicos[350]. En suma, se ha de entender por consentimiento del interesado la autorización libre (otorgada sin coacción ni intimidación), específica (para un determinado tratamiento) e inequívoca (declaración o acción afirmativa[351]) que concede el titular de los datos después de haber sido informado con todos los requisitos legales, para que se realice un tratamiento de los mismos.

En cuanto al objeto del derecho que nos ocupa, el interesado tiene derecho a elegir bajo qué circunstancias y para qué objetivos se pueden tratar sus datos personales[352]. En este segundo sentido, el consentimiento se convierte en su instrumento de control[353]. El consentimiento del interesado se define como en cualquier manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o bien mediante una clara acción afirmativa, el tratamiento de los datos personales que le conciernen[354]. En un primer momento, la Directiva 95/46/CE presentó el consentimiento como "*toda manifestación de voluntad, libre, específica e informada mediante la que el interesado consienta el tratamiento de datos personales que le conciernan*". Al mismo tiempo, el artículo 7.a) añadió el sintagma "consentimiento de forma inequívoca" como modo en que se legitimaba el tratamiento de datos personales[355]. El RGPD ha mantenido la base de la definición que otorgó la Directiva 95/46/CE, pero ha sumado el requisito del consentimiento inequívoco, trasladando el mismo del derogado artículo 7.a) a la definición del artículo 4.11 del RGPD.

---

segundo grupo, se identifica nuevamente el consentimiento expreso del interesado como base legitimadora para el tratamiento.

[350] POLO ROCA, A., "El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado", *Revista de Derecho Político*, Vol. 1, Núm. 108, 2020, p. 187

[351] Esta cuestión ha sido objeto de disputa, aunque, tal y como se analizará más adelante, el actual concepto de "consentimiento inequívoco" ha de comprenderse como una declaración o acción afirmativa.

[352] SCHERMER, B.W.; CUSTERS, B.; VAN DER HOF, S., "The crisis of consent: How stronger legal protection may lead to weaker consent in data protection", *Ethics and Information Technology*, Vol. 16, Núm. 2, 2014, p. 174

[353] MITTAL, S. y SHARMA, P., "The role of consent in legitimising the processing of personal data under the current EU data protection framework", *Asian Journal of Computer Science And Information Technology*, Vol. 7, Núm. 4, 2017, p. 76

[354] Artículo 4.11 RGPD

[355] GT29. Dictamen 15/2011 sobre la definición del consentimiento, 01197/11/ES (WP 187), 13 de julio de 2011, p. 6

Por su parte, el artículo 6.1 de la LOPDGDD entiende por consentimiento del afectado[356] toda manifestación de voluntad libre, específica, informada e inequívoca por la que este acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personas que le conciernen. Es claro que tanto el RGPD como la LOPDGDD se refieren al mismo acto de consentir como base legitimadora del tratamiento de datos, aunque utilicen distintos nombres. Ambas acciones deben ser comprendidas como equivalentes. El artículo 3.e) de la derogada Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal refuerza esta afirmación, puesto que definía como afectado o interesado a la persona que fuese titular de los datos objeto del tratamiento. Aunque la actual norma estatal, la LOPDGDD, se decante por el término del consentimiento del afectado, en ocasiones, se refiere también al "consentimiento del interesado", siendo un claro ejemplo de ello el apartado 2.a) de la Disposición adicional decimoséptima[357].

En su función de base legitimadora, el consentimiento está contemplado como primera de las bases legitimadoras enumeradas en el artículo 6.1 del RGPD que se refiere al tratamiento de cualquier categoría de datos. Por su parte, el artículo 9.1 del mismo cuerpo legal prohíbe el tratamiento de categorías especiales de datos personales entre los que se encuentras los datos relativos a la salud. No obstante, en el apartado 2 del mismo artículo se recogen ciertas circunstancias en las que se permitirá su tratamiento. Por tanto, para poder realizar un tratamiento de los datos personales, se deberá cumplir una de las bases legales del artículo 6.1 del RGPD, y para el caso del tratamiento de los datos relativos a la salud, deberá concurrir una de las situaciones previstas en el artículo 9.2 del RGPD.

El artículo 6.1.a) del RGPD identifica al consentimiento como una de las bases legitimadoras que legitiman el tratamiento de datos personales. El artículo 9.1 de la normativa prohíbe el tratamiento de categorías especiales de datos personales como los datos relativos a la salud. No obstante, en el apartado 2 del mismo artículo se recogen ciertas circunstancias en las que se permitirá su tratamiento. Más concretamente, en el apartado 2.a) se permite el tratamiento de dichos datos siempre y cuando el interesado haya otorgado su consentimiento explícito. Esto es, como norma general, el tratamiento de los datos relativos a la salud está prohibido, pero esta prohibición queda sin efecto cuando el interesado haya otorgado su consentimiento explícito.

El RGPD refuerza el consentimiento para el tratamiento de datos relativo a la salud exigiendo que este consentimiento sea explícito. En relación con lo anterior, en el ámbito sanitario, es necesario diferenciar el concepto del "consentimiento del interesado o afectado" del "consentimiento informado". Veamos, a continuación, en qué consiste la diferencia entre ambas acciones.

---

[356] El LOPDGDD utiliza el término "afectado" en vez de "interesado".

[357] *"**El interesado** o, en su caso, su representante legal podrá otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y, en particular, la biomédica. Tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una* especialidad médica o investigadora."

4.2. Diferenciación de los conceptos "consentimiento del interesado" y "consentimiento informado":

En general, en la normativa relativa a los datos de salud, el concepto "consentimiento informado" es utilizado erróneamente para referirse al "consentimiento del interesado". El primero encuentra su base en el artículo 8 de la Ley 41/2002, de 14 noviembre, Básica Reguladora de la Autonomía del Paciente y de Derechos y Obligaciones en materia de Información y Documentación Clínica[358], en adelante LBAP, y se refiere a la acción por la cual el paciente decide libremente sobre las medidas terapéuticas y tratamientos consintiendo su práctica o rechazándolas. Se trata, como es sabido, de un derecho del paciente, correlativo a un deber del médico.

Por su parte, tal y como se ha expuesto en el punto anterior, el "consentimiento del interesado" contemplado en la normativa de protección de datos, consiste en una de las bases legitimadoras del tratamiento de los datos personales. Debe solicitarlo el responsable del tratamiento, y otorgarlo el interesado. La diferenciación entre los citados conceptos es crucial en el ámbito sanitario conectado, puesto que el objeto del consentimiento varía en uno y otro caso. Nótese que con cada consentimiento el paciente/interesado autoriza un acto distinto; a saber, la aplicación de medidas terapéuticas y tratamientos (consentimiento informado), por una parte, y el tratamiento de sus datos personales sanitarios (consentimiento del interesado), por otra.

La LBAP define en su artículo 3 el consentimiento informado como *"la conformidad libre, voluntaria y consciente de un paciente, manifestada en el pleno uso de sus facultades después de recibir la información adecuada, para que tenga lugar una actuación que afecta a su salud"*. El Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica del País Vasco[359] recoge en su artículo 25.1 que toda actuación en el ámbito de la salud de un o una paciente necesita el consentimiento libre, voluntario e informado de la persona afectada, del que se dejará constancia en la historia clínica.

El Tribunal Constitucional ha interpretado el consentimiento informado del paciente como una facultad de autodeterminación que legitima al paciente, en uso de su autonomía de la voluntad, para decidir libremente sobre las medidas terapéuticas y tratamientos que puedan afectar a su integridad, escogiendo entre las distintas posibilidades, consintiendo su práctica o rechazándolas.

Por lo expuesto, queda demostrado que el consentimiento informado y el consentimiento del interesado son dos figuras distintas[360]. A título ejemplificativo cabe pensar que, si una persona va a participar en un ensayo clínico en el cual se recabarán sus datos relativos a la salud mediante las TIC, deberá otorgar dos consentimientos

[358] BOE núm. 274, de 15 de noviembre de 2002
[359] BOVP núm. 65, de 29 de marzo de 2012
[360] COMISIÓN EUROPEA., "Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation", *health.ec.europa.eu*, disponible en: https://health.ec.europa.eu/system/files/2019-04/qa_clinicaltrials_gdpr_en_0.pdf

distintos antes de que comience dicho ensayo: el consentimiento del interesado para el tratamiento de sus datos relativos a la salud y el consentimiento informado para participar en el ensayo clínico[361]. Lo mismo sucede si el paciente debe someterse a una intervención quirúrgica. Puesto que, por una parte, mediante las nuevas tecnologías se recabarán sus datos relativos a la salud para su posterior análisis, y una vez sean analizados, se procederá a tomar las medidas sanitarias necesarias. Por ello, el participante deberá autorizar previamente el tratamiento de sus datos mediante el consentimiento del interesado. Posteriormente, para que se le apliquen las medidas sanitarias adecuadas que se deduzcan del análisis de los datos, es necesario que otorgue el consentimiento informado.

Para que la facultad de consentir pueda ejercitarse con plena libertad es imprescindible que el paciente cuente con la información médica adecuada sobre las medidas terapéuticas, dado que solo si dispone de dicha información podrá prestar libremente su consentimiento, eligiendo entre las opciones que se le presenten, o decidir, también con plena libertad, no autorizar los tratamientos o las intervenciones que le propongan los facultativos. El consentimiento y la información, como puede verse, se manifiestan como dos derechos tan estrechamente imbricados que el ejercicio de uno depende de la previa correcta atención del otro[362], razón por la cual la privación de información no justificada equivale a la limitación o privación del propio derecho a decidir y consentir la actuación médica, afectando así al derecho a la integridad física del que ese consentimiento es manifestación[363]. La información y el posterior consentimiento están íntimamente vinculados, y dada la relevancia de ese vínculo, surge la denominación "consentimiento informado". Por consiguiente, se comprende que se exija que el paciente otorgue su consentimiento informado antes de que se le aplique o realice un tratamiento o intervención[364].

Para evitar confusiones, es recomendable separar el consentimiento informado y el consentimiento del interesado en dos documentos distintos. Sin embargo, el Reglamento admite que ambos consentimientos se incorporen a un solo documento o acto siempre que haya una diferenciación suficiente que permita al interesado comprender que existen dos objetos distintos sometidos a su consideración sobre los que puede consentir o no.

---

[361] DOVE, E. S., y CHEN, J., "Should consent for data processing be privileged in health research? A comparative legal analysis", *International Data Privacy Law*, Vol. 10, Núm. 2, 2020, p. 128

[362] La STS 948/2011, de 16 de enero de 2012 (Rec. Núm. 2243/2008) analiza las consecuencias de la falta de información ante una intervención quirúrgica, reflejando adecuadamente que el consentimiento y la información deben ir de la mano. El demandante sufrió una tetraplejia grave como consecuencia de una disectomía cervical, no habiendo sido informado adecuada ni suficientemente sobre dicho riesgo con anterioridad a la intervención quirúrgica por el profesional sanitario. El demandante se acogió a la teoría de la pérdida de oportunidad, alegando que el daño sufrido resultaba de la omisión de la información previa al consentimiento. Es decir, que al no informarle de los riesgos que conllevaba la intervención no vital, se le había privado el derecho a tomar una decisión que afectaría a su salud. Véase al respecto: BARCELÓ DOMÉNECH, J., "Consentimiento informado y responsabilidad médica", *Actualidad Jurídica Iberoamericana*, Núm. 8, 2018, p. 291

[363] STC 37/2011, de 28 de marzo de 2011 (BOE núm. 101 de 28 de abril de 2011)

[364] Véase al respecto: PELAYO GONZÁLEZ-TORRE, A., *El derecho a la autonomía del paciente en la relación médica*, Comares, Granada, 2009

Tal y como se ha adelantado más arriba, el consentimiento del interesado para el procesamiento de sus datos ha de ser libre, específico, inequívoco e informado. Se han de cumplir los cuatro requisitos para que el consentimiento otorgado por el interesado se considere válido. Por otra parte, hay que señalar que no es correcto utilizar la denominación de "consentimiento informado" para referirse al acto por el cual el interesado autoriza el tratamiento de sus datos personales, puesto que de dicha manera solo se hace referencia a uno de los requisitos que ha de cumplir el consentimiento para el tratamiento de datos personales. Cuando el consentimiento sea informado se cumplirá una de las exigencias recogidas en la normativa, pero igualmente deberán cumplirse los tres requisitos restantes: libre, específico e inequívoco. Por todo ello, en el presente trabajo de utilizará el concepto "consentimiento del interesado" y no el de consentimiento informado, que reservaremos para referirnos al que emite el paciente en los casos determinados por la LBAP.

4.3. Requisitos del consentimiento del interesado:

La derogada Directiva 95/46 definía en su artículo 2.h) el consentimiento del interesado como toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consentía el tratamiento de datos personales que le concernían. En cambio, tal y como se ha indicado anteriormente, el RGPD lo define como toda manifestación de voluntad libre, específica, informada e inequívoca. Así, mediante la reforma, se incorporó un nuevo requisito ("inequívoco"), pero, al mismo tiempo, se reforzaron los requisitos que ya se recogían en la Directiva. Por tanto, el consentimiento tiene que cumplir cuatro requisitos: ser libre, específico, informado e inequívoco. A continuación, desarrollaremos los citados elementos con el fin de definir en qué consiste el consentimiento válido del interesado en materia de cesión de datos relativos a la salud.

4.3.1. Libertad del consentimiento:

El término "libre" implica elección y control reales por parte del interesado. El consentimiento quedará, por tanto, invalidado por cualquier influencia o presión inadecuada ejercida sobre el interesado que impida que este ejerza su libre voluntad. Para verificar si el consentimiento se ha otorgado de forma libre se han de considerar cuatro elementos: el desequilibrio de poder, la condicionalidad, la granularidad y el perjuicio.

En el Considerando 43 del RGPD se tiene en cuenta el desequilibrio de la relación entre el responsable del tratamiento y el interesado a la hora de valorar si el consentimiento ha sido otorgado libremente o no[365]. En los casos en los que existe un claro desequilibrio entre el responsable del tratamiento y el sujeto interesado, no podrá considerarse que el consentimiento haya sido otorgado con todas las garantías. Precisamente, en la relación médico-paciente, debe constatarse que esta es por

[365] Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, 4 de mayo de 2020, p. 6

antonomasia una relación asimétrica. A modo de ejemplo, podemos citar la referencia del CEPD[366] cuando considera que existirá un desequilibrio siempre que el interesado no se encuentre en buen estado de salud, pertenezca a un grupo desfavorecido desde el punto de vista económico o social o si se encuentra en una situación de dependencia institucional o jerárquica[367]. Por ello, se deberán tomar todas las medidas necesarias para que dicha relación desigual no condicione el consentimiento del interesado.

En cuanto al elemento de la condicionalidad, el consentimiento no debe de vincularse a la aceptación de los términos o condiciones, o "vincular" la prestación de un contrato o servicio a una solicitud de consentimiento para el tratamiento de datos personales que no sean necesarios para la ejecución de dicho contrato o servicio. Si el consentimiento se da en esta situación, se presume que no se da libremente. Siempre que una solicitud de consentimiento esté vinculada a la ejecución de un contrato o prestación de un servicio, el interesado que no desee poner sus datos personales a disposición del responsable del tratamiento corre el riesgo de que se le nieguen los servicios que ha solicitado, quebrantándose la opción de libertad genuina para dar su consentimiento[368]. Por ejemplo, si un proveedor de sitios web introduce un recuadro que oculta el contenido y no es posible acceder al contenido sin pulsar el botón "aceptar las cookies", el interesado no manifestará un consentimiento libre, dado que no se le ofrece una posibilidad real de elección. No estaríamos ante un consentimiento válido, ya que solo se prestará el servicio si el interesado pulsa el citado botón[369].

La expresión "necesario para la ejecución de un contrato" del artículo 7.4 del RGPD debe ser interpretada de manera restrictiva[370]. El responsable del tratamiento debe ofrecer una opción real y libre de consentir a los tratamientos adicionales que conlleva la ejecución de un contrato o prestación de un servicio, sin que en ningún momento la

[366] El CEPD (EDPS en inglés) es un organismo de la Unión Europea que sustituyó al GT29. Se trata de un organismo independiente que asesora a la Comisión Europea en materia de protección de datos personales. Supervisa la aplicación del RGPD dentro de la Unión Europea, así como en Noruega, Liechtenstein e Islandia, sin perjuicio de las competencias de las autoridades de control. El CEPD celebra reuniones periódicas en Bruselas para debatir y tomar decisiones sobre cuestiones relativas a la protección de datos. Las decisiones son adoptadas en las reuniones plenarias a las que asisten los responsables de las autoridades nacionales, sobre la base del trabajo previo de las reuniones de los subgrupos de expertos y de la secretaría del CEPD. Esta figura se regula en los artículos 68-201 del RGPD.

[367] CEPD. Dictamen 3/2019 sobre las preguntas y respuestas acerca de la relación entre el Reglamento sobre ensayos clínicos (REC) y el Reglamento general de protección de datos (RGPD) artículo 70, apartado 1, letra b), 23 de enero de 2019, p.7

[368] GESTADATA CONSULTING., El consentimiento según el RGPD, *gestadataconsulting*, 31 de julio de 2020, disponible en: https://www.gesdataconsulting.es/consentimiento-segun-el-rgpd/ *[Última consulta: 9 de junio de 2021]*

[369] CEPD. Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, *cit.*, p. 11

[370] Mediante el procedimiento sancionador 46/2019, de 25 de noviembre de 2019, la AEPD sancionó a una escuela de baile por incluir en la hoja de la matrícula la autorización a la captación de imágenes de los alumnos, no existiendo posibilidad de no otorgar dicho consentimiento *y* haciéndolo dependiente de la matriculación: "*La circunstancia de incluir de modo obligatorio para los padres/alumnos en el impreso de matrícula la cesión de la imagen para los fines que se contienen o la del envío publicitario no se ajustan al RGPD ni a la base legitimadora del consentimiento, al incluirse y mezclarse con la base legitimadora contractual y debiendo aceptar esta. Es decir, se tiene que dar la aceptación al bloque, por lo que no puede considerarse consentimiento como manifestación de voluntad libre*".

negativa del interesado afecte a la ejecución del contrato o la prestación de servicio solicitado por el mismo. La obligación de autorizar el uso de datos personales más allá de lo estrictamente necesario limita las opciones del interesado y le impide ejercer su libre consentimiento. Dar el consentimiento a un tratamiento de datos personales que no sea necesario no puede considerarse como un requisito obligatorio para la ejecución de un contrato o la prestación de un servicio. Se pretende con esto garantizar que el tratamiento de los datos personales no se camufle o se vincule a la prestación de un contrato o servicio para el cual dichos datos personales no son necesarios[371]. Para evaluar si tiene lugar esa situación de vinculación o supeditación, es importante determinar el alcance del contrato y qué datos serían necesarios para la realización de dicho contrato.

El citado artículo solo se aplica cuando los datos solicitados no son necesarios para la ejecución del contrato (incluida la prestación de un servicio), y la ejecución de dicho contrato se condiciona a la obtención de esos datos sobre la base del consentimiento. Por el contrario, si el tratamiento es necesario para la ejecución del contrato (inclusive para la prestación de un servicio) entonces el artículo 7, apartado 4, no será de aplicación. De este modo, el RGPD trata de garantizar que el tratamiento de los datos para los que se ha solicitado consentimiento no se convierta directa o indirectamente en una contraprestación de un contrato[372]. Es necesario prestar la debida atención a si la aceptación de los términos y condiciones que son objeto del consentimiento están "agrupadas" o si el consentimiento se encuentra innecesariamente "vinculado" a la provisión de un contrato o un servicio cuando los datos personales solicitados no resultan necesarios para ejecutar o cumplir el contrato o prestar efectivamente el servicio[373]. Para evaluar si tiene lugar esa vinculación, resulta necesario determinar el alcance del contrato o servicio y que datos serían necesarios para la realización del mismo[374]. Si existe este agrupamiento o vinculación, podrá llegar a considerase que el consentimiento se encuentra condicionado a una contraprestación ilegítima, como es la cesión de datos a cambio de la prestación del servicio, y por tanto que no ha sido prestado libremente[375]. En interpretación del RGPD se ha dicho que, cuando se solicita el consentimiento como condición previa de (y no relacionada con) el servicio que se

[371] STJUE (Gran Sala) de 1 de octubre de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801, apartado 97
[372] GT29. Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 (WP 259), *cit.*, p.9
[373] TJUE (Gran Sala), Conclusiones del abogado general, de 21 de marzo de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801, apartado 97: *"al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio,* ***se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato****. Por consiguiente, el artículo 7, apartado 4, del Reglamento 2016/679 establece una «prohibición de prácticas de consentimiento agrupado»".*
[374] BERROCAL LANZAROT, A. I., *Estudio jurídico-crítico sobre la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales: análisis conjunto del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 y de la Ley Orgánica 3/2018 de 5 de diciembre*, Reus, Madrid, 2019, p. 227
[375] IBERLEY., "Condiciones del consentimiento en materia de protección de datos en el Reglamento General de Protección de Datos (RGPD) y en la LO 3/2018 (LOPDGDD)", *iberley*, 30 de enero de 2019, disponible en: https://www.iberley.es/temas/condiciones-aplicables-consentimiento-materia-proteccion-datos-62815 *[Última consulta: 10 de junio de 2021]*

presta, aunque se preste el consentimiento este será inválido por no haberse prestado con plena libertad[376].

GARCIA RIPOLL afirma que, a pesar del artículo 7.4 RGPD, las Directrices sobre el consentimiento y las insinuaciones de la STJUE 1 octubre 2019 (C-673/17), sí que se puede condicionar el acceso a servicios en internet (o en otro ámbito) a que el interesado ceda algunos datos personales, puesto que, según el autor, el papel de regular el consentimiento contractual, en que los datos se ceden a cambio de otra prestación, se ha dejado a la Directiva 2019/770, sobre contratos de suministro de contenidos y servicios digitales[377]. En contra de esta afirmación cabe alegar que en el Considerando 38 de la citada Directiva se recoge lo siguiente:

> *"La presente Directiva* ***no debe regular las condiciones para el tratamiento lícito de datos personales, por cuanto esta cuestión está regulada, en particular, por el Reglamento (UE) 2016/679****. Por consiguiente,* ***todo tratamiento de datos personales en relación con un contrato que entre en el ámbito de aplicación de la presente Directiva solo es lícito si es conforme a lo dispuesto en el Reglamento (UE) 2016/679*** *en relación con los fundamentos jurídicos para el tratamiento de los datos personales. Cuando el tratamiento de datos personales esté basado en* ***el consentimiento****, en particular con arreglo al artículo 6, apartado 1, letra a), del Reglamento (UE) 2016/679,* ***son de aplicación las disposiciones específicas de dicho Reglamento, incluidas las relativas a las condiciones para valorar si el consentimiento se presta libremente****."*

Por consiguiente, en base a los Considerandos 42 y 43 y al artículo 7.4 del RGPD, para que el consentimiento del interesado sea lícito, se deberá cumplir el requisito de la libertad en todos los casos sin excepción alguna.

En este mismo sentido, la AEPD indicó en interpretación de la normativa española que la instalación y utilización de un aplicativo no puede estar condicionada a la obtención de un consentimiento para un tratamiento no necesario para proporcionar el servicio definido en la misma[378]. Por ejemplo, si una persona mayor quiere descargarse una aplicación para controlar el ejercicio diario que realiza, para que la aplicación funcione, el usuario deberá activar su localización GPS. Sin embargo, si a la hora de descargarse la aplicación en cuestión la misma solicita que el usuario active el micrófono del teléfono y no se completa la descarga hasta que lo autorice, el consentimiento otorgado por el usuario no será libre. El micrófono no es necesario para calcular la distancia

---

[376] GARCÍA PÉREZ, R.M., "Bases jurídicas relevantes del tratamiento de datos personales en la contratación de contenidos y servicios digitales", *Cuadernos de derecho transnacional*, Vol. 12, Núm. 1, 2020, p. 894

[377] GACÍA RIPOLL MONTIJANO. M., "El consentimiento al tratamiento de datos personales", en GONZÁLEZ PACANOWSKA, I. y CASTILLA BAREA, M., *Protección de datos personales*, Tirant lo Blanch, 2020, p. 155

[378] AEPD., "El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles", *aepd*, 17 de septiembre de 2019, p. 2, disponible en: https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf

recorrida por el usuario, es decir, el tratamiento de esos datos no es necesario para la prestación de dicho servicio, va más allá de lo necesario. Dado que el usuario no puede utilizar la aplicación sin consentir que el micrófono se active, el consentimiento se convierte en una contraprestación del contrato. Si en cambio el usuario ha activado el micrófono y por consiguiente se ha descargado la aplicación, y posteriormente retira el consentimiento, puede que la aplicación no funcione en su totalidad, así en base al Considerando 42 del RGPD, el consentimiento no será libre, puesto que el interesado no puede retirar su consentimiento sin sufrir perjuicio alguno.

El tercer elemento constitutivo de la validez del consentimiento del interesado es la identificación del propósito o de la finalidad. Se presume que el consentimiento no se ha dado libremente cuando se impide o dificulta el autorizar por separado las distintas operaciones de tratamiento de datos personales, pese a ser adecuado en el caso concreto[379]. Si el responsable del tratamiento ha combinado varios propósitos para el procesamiento y no ha solicitado un consentimiento por separado para cada propósito, existe una falta de libertad. Esto es, el consentimiento no será libre cuando no se le permita al interesado autorizar por separado los distintos tratamientos de datos personales. La así llamada granularidad está estrechamente relacionada con la necesidad de que el consentimiento sea específico, requisito que se analizará posteriormente. Para que el consentimiento sea válido, la solución radica en la separación de estos propósitos y la obtención del consentimiento para cada uno de los mismos.

Por último, debemos referirnos al elemento de la libertad del consentimiento sin perjuicio de los derechos o intereses del interesado. Si el interesado no puede negar o retirar su consentimiento sin perjuicio, el consentimiento no será libre[380]. El interesado debe tener la posibilidad de negar o retirar el consentimiento sin sufrir perjuicio alguno[381]. El responsable del tratamiento debe poder demostrar que la retirada del consentimiento no conllevará ningún coste para el interesado y, por tanto, ninguna clara

[379] Considerando 43 RGPD

[380] Por motivo de la situación de crisis sanitaria ocasionada por el COVID-19 una universidad consultó a la AEPD una serie de cuestiones relativas al uso de técnicas de reconocimiento facial en la realización de pruebas de evaluación online. En la consulta se alegaba que uno de los tratamientos usuales durante la realización de un examen consiste en la verificación de la identidad de la persona examinada, ya sea a la entrada en el aula, durante la realización de la prueba o al final de la misma a la entrega de la documentación. Para ello, se exige la exhibición de un documento identificativo, DNI, tarjeta de residencia, pasaporte, o carné universitario. Sin embargo, como dicha comprobación de la identidad no es posible en un examen online, se consultaba la posibilidad de utilizar una herramienta de reconocimiento facial. La AEPD resolvió que la posibilidad de admitir un consentimiento libre de los alumnos que permitiera el empleo de técnicas de reconocimiento facial al objeto de tratar sus datos biométricos en las evaluaciones online requeriría que a los mismos se les ofreciera la posibilidad de realizar dichas evaluaciones en una situación equiparable en la que no fuera necesario su tratamiento, como pudiera ser la realización de la misma actividad presencialmente, u ofreciendo otras alternativas que no requieran el tratamiento de sus datos biométricos y que fueran equiparables en cuanto a su duración y dificultad a las que se realicen mediante el empleo del reconocimiento facial. En caso contrario, el consentimiento no podría considerarse libremente prestado. Lo que no sería admisible, en ningún caso, es que como consecuencia de la denegación del consentimiento se denegara la posibilidad de matriculación o de acceder a la evaluación o cualquier otra consecuencia negativa importante para el alumno. Véase al respecto: AEPD. Informe jurídico núm. 0036/2020 de 8 de mayo de 2020, p. 25

[381] Considerando 42 del RPGD

desventaja para quienes retiren el consentimiento. Otros ejemplos de prejuicio son el engaño, la intimidación, la coerción o consecuencias negativas importantes si un interesado no da su consentimiento. Ligando este elemento al de la responsabilidad, corresponde al responsable del tratamiento debe ser capaz de demostrar que el interesado pudo ejercer una elección libre o real a la hora de dar su consentimiento y que le era posible retirarlo sin sufrir ningún perjuicio[382].

4.3.2. La especificidad como requisito del consentimiento:

Para que el consentimiento pueda considerarse específico, el responsable del tratamiento debe especificar el fin del tratamiento como garantía contra la desviación del uso, además tiene que separar las solicitudes de consentimiento, y finalmente, ha de diferenciar la información para las actividades de tratamiento de datos personales y la información relativa a otras cuestiones[383]. Con estas tres acciones se pretende garantizar un nivel de control y transparencia para el interesado, dando opción a este a elegir con respecto a cada uno de dichos fines y una garantía contra la desviación del uso[384]. El consentimiento debe tener concretamente por objeto el tratamiento de datos de que se trate y no puede deducirse de una manifestación de voluntad que tenga un objeto distinto[385].

Respecto a la especificación del fin del tratamiento, el artículo 5.1.b) del RGPD establece que los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines[386]. Por su parte, el Considerando 50 del mismo cuerpo legal recoge que el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. Por tanto, debemos entender que el principio de limitación de la finalidad implica, por una parte, la obligación de que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas y, por otra, supone la prohibición de que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines[387].

---

[382] GT29, Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 (WP 259), 10 de abril de 2018, p. 11-12

[383] Ibid., pp.13-14

[384] POLO ROCA, A., "El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado", *cit.*, p. 185

[385] STJUE (Gran Sala), de 1 de octubre de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801, apartado 58.

[386] STJUE (Sala Primera), de 20 de octubre de 2022, Digi Távközlési és Szolgáltató Kft contra Nemzeti Adatvédelmi és Információszabadság Hatóság, asunto C-77/21, ECLI:EU:C:2022:805

[387] AEPD., "Principios", *aepd*, 30 de agosto de 2019, disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios#:~:text=Principio%20de%20%E2%80%9C%20limitaci%C3%B3n%20de%20la,leg%C3%ADtimos%20sean%20tratados%20posteriormente%20de *[Última consulta: 12 de junio de 2021]*

Se ha afirmado que la evolución tecnológica pone en cuestión el principio de limitación de la finalidad[388]. Así, el procesamiento de datos en masa (Big Data) a menudo no tiene un propósito fijo, y el uso potencial de los datos se llega a vislumbrar una vez recopilados y tratados los datos en base a combinaciones aleatorias[389]. Según esta opinión, no es posible saber de antemano que tratamiento puede realizarse, y para averiguarlo, es necesario recopilar todos los datos posibles y posteriormente deducir cuáles son los realmente relevantes[390]. Pero lo cierto es que el uso de datos sin finalidad inicial explícita contraria al RGPD, dado que dejaría sin valor tanto el principio de limitación de la finalidad como el principio de minimización de datos. No obstante, en el ámbito de la investigación científica, la normativa permite otorgar consentimientos amplios.

En cuanto a la exigencia de compatibilidad, el artículo 5.1.b) del RGPD recoge que, de acuerdo con el artículo 89.1 del mismo cuerpo legal, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales. En este aspecto, se ha seguido la línea del derogado principio de calidad que se preveía en el artículo 4 del LOPD, el cual establecía en su punto segundo que los tratamientos posteriores de datos con finalidades históricas, estadísticas o científicas no eran incompatibles.

Por tanto, el tratamiento ulterior de los datos personales con fines de archivo, fines de investigación científica e histórica o fines estadísticos, no se considerará, incompatible con los fines iniciales, siempre que se produzca de conformidad con las disposiciones del artículo 89 del RGPD, que prevé garantías y excepciones específicas. En tal caso, el responsable del tratamiento podrá, en determinadas condiciones, realizar el tratamiento ulterior de los datos sin necesidad de una nueva base jurídica[391]. En este sentido, tal y como se desarrollará más adelante, en el apartado 2.c) de la Disposición Adicional decimoséptima se dispone que se considerará lícita y compatible la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. Esto es, no se solicitará de nuevo el consentimiento si los datos se utilizan para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. Por todo ello, este tratamiento secundario de los datos no consentido específicamente por el interesado, pero será

[388] MOEREL, L. y PRINS, C., "Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things", *Tilburg University*, 2016, p. 6, disponible en: http://dx.doi.org/10.2139/ssrn.2784123

[389] VAN DER SLOOT, B. Y VAN SCHENDEL, S., "Ten Questions for the Future Regulation of Big Data: A Comparative and Empirical Legal Study", *JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 7, 2016, p. 119

[390] HILDEBRANDT, M., "Slaves to big data. Or are we?", IDP *Revista de Internet, Derecho y Política*, núm. 17, 2013, p. 15

[391] CEPD. Dictamen 3/2019 sobre las preguntas y respuestas acerca de la relación entre el Reglamento sobre ensayos clínicos (REC) y el Reglamento general de protección de datos (RGPD) [artículo 70, apartado 1, letra b)], *cit.*, p.9

legítimo siempre y cuando esté relacionado con el área en la que se integraba científicamente el estudio inicial (uso primario de los datos personales).

De este modo, el RGPD diferencia los tratamientos posteriores compatibles de los tratamientos incompatibles. Los datos personales podrán ser tratados con fines distintos de aquellos para los que hayan sido recogidos inicialmente siempre que este nuevo fin sea compatible con el inicial. Esto es, se permite el tratamiento posterior de los datos para otro fin que no sea incompatible con el inicial. En lugar de imponer un requisito de compatibilidad, el legislador ha optado por una doble negación prohibiendo la incompatibilidad. De esta forma, se concluye que cualquier tratamiento posterior está autorizado siempre que no sea incompatible y si los requisitos de legalidad también se cumplen simultáneamente. El hecho de que el procesamiento posterior tenga un propósito diferente no significa necesariamente que sea automáticamente incompatible, sino que dicho juicio debe realizarse caso por caso[392]. Mediante esta posibilidad de realizar un tratamiento posterior de datos para un fin distinto, el legislador ha querido permitir que el principio de limitación de la finalidad del artículo 5.1.b) no sea tan inflexible. La prueba de compatibilidad proporciona una exención de facto al principio de limitación de la finalidad, lo que permite una mayor flexibilidad de procesamiento para usos secundarios[393].

En cualquier caso, esta flexibilización del principio de limitación de la finalidad no exime al responsable del tratamiento de informar al interesado con anterioridad al tratamiento ulterior sobre el nuevo fin y cualquier información adicional pertinente en base a los artículos 13.3 y 14.4 del RGPD. El RGPD establece un deber adicional para el responsable del tratamiento al imponer la obligación de informar al interesado cuando proyecte el tratamiento ulterior de los datos para un fin que no sea aquel para el que se recogieron. El apartado 2.c) de la Disposición Adicional decimoséptima recoge igualmente este deber adicional de información al disponer que, en caso de compatibilidad, los responsables deberán publicar la información establecida por el artículo 13 del RGPD en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos últimos carezcan de medios para acceder a tal información, podrán solicitar su remisión en otro formato.

Como se viene afirmando, el responsable del tratamiento debe limitar el tratamiento de los datos a una o varias finalidades determinadas, explícitas y legítimas. Una vez que se haya otorgado el consentimiento por parte del titular de los datos y se haya procedido a la recolección de los mismos en base al fin o fines estipulados, no se podrá realizar ningún tratamiento posterior incompatible a dicho fin o fines. Esta prohibición funciona como garantía para evitar una ampliación espuria de los fines para los que se realiza el

[392] GT29. Opinión 3/2013 sobre la limitación de la finalidad (WP 203), de 2 de abril de 2013, p. 21

[393] COMANDE,G. y SCHNEIDER,G., "Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of Health Data", *European Journal of Health Law*, Vol. 25, Núm. 3, 2017, p. 303

tratamiento de los datos una vez que un interesado haya dado su autorización a la recogida inicial de los datos. Este fenómeno, también conocido como desviación del uso, supone un riesgo para los interesados ya que puede dar lugar a un uso imprevisto de los datos personales por parte del responsable del tratamiento o de terceras partes y a la pérdida de control por parte del interesado[394].

Asimismo, dado que, cuando el tratamiento de los datos personales tenga como base legitimadora el consentimiento del interesado, este deberá ser otorgado para un solo fin específico, el responsable del tratamiento debe separar o desglosar las solicitudes de consentimiento para cada fin. Si se proyectase más de un fin para el tratamiento de los datos, no es suficiente con un consentimiento general que cubra todos los tratamientos de datos, sino que deben separarse por finalidades. Por ello, tal y como se ha adelantado antes, los mecanismos de consentimiento no solo deben ser granulares para cumplir el requisito de "libre", sino también para cumplir el requisito de "específico". No obstante, como referiremos en el capítulo dedicado al tratamiento de los datos relativos a la salud con fines de investigación en salud, existen posiciones doctrinales encontradas en cuanto al grado de explicitación exigible al responsable del tratamiento cuando se trata de obtener el consentimiento para el tratamiento de los datos en materia de investigación.

Un responsable del tratamiento que busque el consentimiento para varios fines distintos, debe facilitar la posibilidad de optar por cada fin, de manera que los usuarios puedan dar consentimiento específico para fines específicos[395]. Por ejemplo, si la finalidad del tratamiento es la prestación de un servicio determinado, no se podrán utilizar los datos con finalidades de marketing salvo que se haya solicitado igualmente el consentimiento para dicha finalidad. Por todo ello, cuando el tratamiento de datos se funde en el consentimiento del interesado para una pluralidad de finalidades, será preciso que conste de manera específica que dicho consentimiento se otorga para cada una de ellas.

Por último, hay que subrayar que el responsable del tratamiento deberá separar la información para las actividades de tratamiento de datos personales y la información relativa a otras cuestiones[396]. Esta obligación del responsable, cobra especial importancia en el ámbito sanitario, donde se deberá separar la información relativa al tratamiento de los datos del resto de la información relativa al tratamiento sanitario con el objetivo de evitar cualquier confusión.

4.3.3. La información debida al interesado:

El interesado debe ser informado sobre todos aquellos elementos que son necesarios para que este pueda formar su voluntad y decidir si consiente el tratamiento de sus datos

[394] GT29, Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 (WP 259), *cit.*, p. 13
[395] Ibid., p. 14
[396] STJUE (Sala Segunda), de 29 de julio de 2019, Fashion ID, C-40/17, ECLI:EU:C:2019:629

personales o no[397]. En este sentido, el Tribunal Constitucional ha declarado que el deber de información previa forma parte del contenido esencial del derecho a la protección de datos, pues resulta un complemento indispensable de la necesidad de consentimiento del afectado. Por ello, a la hora de valorar si se ha vulnerado el derecho a la protección de datos por incumplimiento del deber de información, la dispensa del consentimiento al tratamiento de datos en determinados supuestos debe ser un elemento a tener en cuenta dada la estrecha vinculación entre el deber de información y el principio general de consentimiento[398].

El artículo 13 del RGPD recoge la información que deberá facilitarse cuando los datos personales se obtengan directamente del interesado[399], y el artículo 14 del RGPD del mismo cuerpo legal la información que deberá facilitarse cuando los datos no se obtengan del interesado[400]. Los citados dos artículos requieren, al menos, la siguiente información: la identidad del responsable del tratamiento y, en su caso de su representante; los datos de contacto del delegado de protección de datos; los fines del tratamiento de los datos personales; en su caso, el interés legítimo del responsable o de un tercero; los destinatarios de los datos personales y la información sobre los posibles riesgos de transferencia de datos debido a la ausencia de una decisión de adecuación y de garantías adecuadas.

A su vez, para que el tratamiento sea considerado leal y transparente, en el momento en que se obtengan los datos personales, el responsable del tratamiento deberá facilitar al interesado la siguiente información: el plazo durante el cual se conservarán los datos personales; los derechos que tiene como interesado (acceso, rectificación, supresión, limitación del tratamiento, oposición y portabilidad de los datos); la existencia del derecho a retirar el consentimiento; el derecho a presentar una reclamación ante una autoridad de control; si la comunicación de los datos personales es un requisito legal o contractual y la información sobre el uso de los datos para decisiones automatizadas. Asimismo, el Comité Europeo de Protección de Datos, en adelante CEPD, señala que, dependiendo de las circunstancias y el contexto de un caso, puede requerirse más información para que el interesado entienda realmente las operaciones de tratamiento que van a tener lugar[401].

Si la información se obtiene del propio interesado, esta información deberá otorgarse en el momento en que se soliciten los datos. Sin embargo, si la información no se obtiene

[397] AEPD., "Informe sobre políticas de privacidad en internet", *aepd*, septiembre de 2018, p. 15, disponible en: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf

[398] STC 39/2016 de 3 de marzo de 2016 (BOE núm. 85 de 8 de abril de 2016)

[399] En relación con el artículo 13 del RGPD, el artículo 11.2. de la LOPDGDD recoge que la información básica deberá contener, al menos: la identidad del responsable del tratamiento y de su representante, en su caso; la finalidad del tratamiento y la posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del RGPD.

[400] En relación con el artículo 14 del RGPD, el artículo 11.3. de la LOPDGDD recoge que la información básica incluirá también las categorías de datos objeto de tratamiento y las fuentes de las que procedieran los datos.

[401] CEPD., Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, 4 de mayo de 2020, p. 15

del propio interesado, el responsable del tratamiento deberá cumplir con su obligación de informar dentro de un plazo razonable, pero en cualquier caso dentro de un mes. Este plazo máximo de un mes no será aplicable cuando exista la obligación de informar con anterioridad por concurrir alguna de las dos siguientes causas: los datos han de utilizarse para comunicarse con la persona interesada o si está previsto comunicarlos a otro destinatario. En el primer caso, se debe informar antes o en el momento de comunicarse con el interesado. En el segundo caso, se debe informar antes o en la primera comunicación[402]. Todos los responsables han de cumplir con esta obligación con independencia de su tamaño como organización.

Una vez expuestos los fundamentos de la información debida al interesado, remitimos en este punto al epígrafe posterior relativo a la información debida al interesado mayor que será objeto de atención específica más adelante.

4.3.4. Consentimiento inequívoco:

El RGPD requiere una declaración del interesado o una clara acción afirmativa como forma de manifestación del consentimiento[403], lo que significa que el consentimiento debe prestarse mediante una acción o declaración (artículo 4.11 del RGPD).

Para que el consentimiento se otorgue de forma inequívoca, el procedimiento de su obtención y otorgamiento no tiene que dejar ninguna duda sobre la intención del interesado al dar su consentimiento[404]. En otras palabras, la manifestación mediante la cual el interesado consiente no debe dejar lugar a ningún equívoco sobre su intención. Si existe una duda razonable sobre la intención de la persona se producirá una situación equívoca.

El interesado debe realizar una declaración verbal[405], por escrito o incluso por medios electrónicos. Esto puede incluir marcar una casilla de un sitio web en internet, escoger

---

[402] APDCAT. Guía para el cumplimiento del deber de informar en el RGPD, 10 de diciembre de 2018, p. 4

[403] Artículo 4.11 del RPGD

[404] STJUE (Gran Sala) de 1 de octubre de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801, apartado 54: "*el consentimiento del interesado puede hacer que tal tratamiento se considere lícito siempre que dicho consentimiento haya sido dado «de forma inequívoca» por el interesado. Pues bien, solo un comportamiento activo por parte del interesado con el que manifieste su consentimiento puede cumplir este requisito".*

[405] En el procedimiento sancionador núm. PS/00307/2018 de 8 de mayo de 2018 de la AEPD, SEGURCAIXA ADESLAS, S.A. de SEGUROS Y REASEGUROS fue sancionada por realizar un tratamiento de datos personales sin el consentimiento inequívoco del interesado. El denunciante recibió una llamada telefónica, en la que le ofrecían la contratación de una póliza de seguro dental y, aunque manifestó su rechazo, ante la insistencia de la interlocutora, indicó que le remitiera la documentación a su domicilio sin ningún compromiso por su parte. A finales del mes de enero, recibió en su domicilio el contrato de seguro dental, la orden de domiciliación bancaria y la tarjeta de asegurado de ADESLAS con sus datos personales y en el mes de marzo, ADESLAS cargó en su cuenta bancaria un recibo por importe de 10,50 €, donde constaban sus datos y los de su esposa como titulares de la cuenta bancaria. Al contactar con ADESLAS para manifestar que no había suscrito ningún contrato, le comunicaron que sus datos bancarios habían sido obtenidos de MUTUA MADRILEÑA ya que ambas entidades formaban parte del mismo grupo empresarial y el denunciante era cliente de MUTUA MADRILEÑA como titular de una póliza de seguro de automóvil. La AEPD resolvió que "*se puede indicar que hay un*

parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente que el interesado acepta la propuesta de tratamiento de sus datos personales. El silencio, las casillas previamente marcadas[406] o la inactividad no deben constituir un consentimiento[407]. En este mismo sentido, el CEPD ha establecido que seguir navegando en la web en ningún caso satisfará la exigencia de una clara acción afirmativa, por lo que no será posible determinar con dicha acción que se ha obtenido un consentimiento inequívoco del interesado[408]. Se requiere una manifestación o acción positiva por parte del interesado. Por tanto, no se acepta el consentimiento tácito o implícito[409]. La RAE define el adjetivo tácito como "callado, silencioso" o "que no se entiende, percibe, oye o dice formalmente, sino que se infiere"[410]. Por consiguiente, el consentimiento tácito es un consentimiento de carácter presunto que no se deduce de actuaciones, sino de la inactividad, del silencio o de la falta de oposición[411]. El RGPD al utilizar la expresión "acto afirmativo" imposibilita la aplicación del consentimiento tácito[412].

Aunque el consentimiento del interesado requiere una declaración o una clara acción afirmativa, en función del grado de sensibilidad del dato en cuestión, se requiere un consentimiento explícito. En base al artículo 9.2 a) del RGPD, es necesario el consentimiento explícito del interesado para el tratamiento de datos personales que

---

consentimiento en el que se recogen los datos, pero no se consiente en la prestación del servicio que queda en estudiar el denunciante y por tanto la emisión de las facturas a la cuenta bancaria del denunciante por un servicio no suscrito, constituyendo un tratamiento de datos sin consentimiento y sin base jurídica en ese punto en concreto. Las alegaciones de la denunciada que se perfección el contrato con el consentimiento del denunciante chocan frontalmente con lo recogido en la conversación telefónica, que aunque sigue un protocolo en la obtención de los datos, no acredita el consentimiento inequívoco del afectado, sino lo contrario por las manifestaciones del afectado e insistencia de la comercial en que le envía los documentos aunque proceda ordenadamente a la lectura de la policita y explicación de la oferta. Por consiguiente, el consentimiento otorgado para el tratamiento de los datos de carácter personal en relación con un concreto envío de documentación o relación pre- contractual no autoriza al responsable del tratamiento a realizar actos de tratamiento de tales datos ajenos a la finalidad para la que se prestó aquel consentimiento, actos post contractuales y que en este caso se concretan en la emisión de dos recibos a la cuenta del denunciante, cuando queda claro en la conversación que quería analizar la oferta".

[406] STJUE (Gran Sala) de 1 de octubre de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801, apartado 52: *"el consentimiento dado mediante una casilla marcada por defecto no implica un comportamiento activo por parte del usuario de un sitio de Internet".*

[407] Considerando 32 del RGPD

[408] EDPB., Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, *cit.*, pp. 18-19

[409] El Real Decreto 1720/2007, de 21 de diciembre, por el que se aprobaba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RDLOPD) admitía el consentimiento tácito en su artículo 14.2*: "El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que* ***en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal****".*

[410] RAE., Definición del adjetivo tácito, disponible en: https://dle.rae.es/t%C3%A1cito *[Última consulta: 13 de junio de 2021]*

[411] APARICIO SALOM, J. y VIDAL LASO, M., *Estudio sobre la protección de datos*, Aranzadi, Pamplona, 2019, p. 162

[412] LINARES GUTIÉRREZA, A., "El consentimiento en los contratos telefónicos de prestación de servicios de comunicaciones ante la nueva regulación sobre protección de datos personales", *Revista Internacional Jurídica y Empresarial*, núm. 2, 2019, p. 145

revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y para el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud[413] o datos relativos a la vida sexual o la orientación sexual de una persona física. Al igual que para el tratamiento de categorías especiales de datos personales, el RGPD requiere el consentimiento explícito del interesado para la transferencia de datos a terceros países u organizaciones internacionales cuando no existan garantías adecuadas y la toma de decisiones individuales automatizadas, incluida la elaboración de perfiles[414].

Por tanto, para dichos tratamientos, el consentimiento además de ser inequívoco deberá ser explícito. El consentimiento explícito consiste en una declaración activa, clara e inequívoca del interesado que acepta o consiente el tratamiento de datos conforme a las condiciones que se le describen, mediante la expresión de su voluntad, que podrá ser por escrito, verbalmente, mediante comunicación telemática o por cualquier otro medio[415].

La LOPDGDD por su parte, recoge una serie de circunstancias en las que el interesado deberá otorgar un consentimiento expreso. Por una parte, en el ámbito de la función estadística pública, la recolección de las categorías especiales de datos personales y los datos personales relativos a condenas e infracciones penales se realizará únicamente si el interesado ha otorgado previamente su consentimiento expreso[416]. Asimismo, en el caso de los datos relativos a la salud, al configurarse los mismos como categorías especiales de datos personales, se requerirá un consentimiento expreso para proceder a su recolección para fines estadísticos públicos. De la misma manera, respecto al acceso a la información pública, si la información que se solicita contiene datos personales que revelen la ideología, afiliación sindical, religión o creencias, el acceso únicamente se podrá autorizar en caso de que se cuente con el consentimiento expreso y por escrito del afectado, salvo que dicho afectado haya hecho manifiestamente públicos los datos con anterioridad a que se solicite el acceso. Si la información incluye datos personales que hagan referencia al origen racial, a la salud o a la vida sexual, incluye datos genéticos o biométricos o contiene datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquel estuviera amparado por una norma con rango de ley[417].

---

[413] En relación directa con esta cuestión, la Autoridad nacional portuguesa competente en materia de protección de datos impuso una multa de 400.000 euros a un hospital por permitir el acceso indebido por parte de profesionales sanitarios a historias clínicas de pacientes sin su consentimiento expreso. Véase al respecto: CABALLERO TRENADO, L., "Primera multa post RGPD en Portugal", *legaltoday*, 29 de noviembre de 2018, disponible en: https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/primera-multa-post-rgpd-en-portugal-2018-11-29/ *[Última consulta: 13 de junio de 2021]*

[414] Considerando 51, 71 y 111; y los artículos 9.2.a), 22.2.c) y 49.1.a) del RGPD

[415] APARICIO SALOM, J. y VIDAL LASO, M., *Estudio sobre la protección de datos, cit.*, p. 151

[416] Artículo 25.2 de la LOPDGDD

[417] Disposición final undécima de la LOPDGDD

Como se ha puesto de manifiesto más arriba, existe una diferencia de denominación entre el RGPD que utiliza el término "consentimiento explícito" y el LOPDGDD que se refiere al "consentimiento expreso". No obstante, la doctrina entiende que las expresiones referidas han de comprenderse como sinónimas. Así, se ha dicho que el término "explícito" se refiere a la manera en que el interesado expresa el consentimiento, y significa que el interesado debe realizar una declaración expresa de consentimiento[418]. Esta declaración expresa será clara, patente y especificada. Debe poder demostrarse que fue el interesado quien otorgó el consentimiento, e identificarse claramente que es lo que consintió. Por consiguiente, el consentimiento expreso debe ser verificable[419].

Una manera de garantizar que el consentimiento sea explícito consiste en plasmar dicho consentimiento en una declaración escrita. Así, el responsable podrá asegurarse de que el interesado firma la declaración escrita con el fin de eliminar cualquier posible duda o falta de prueba en el futuro. Sin embargo, dicha declaración firmada no es el único modo de obtener el consentimiento explícito, el RGPD no prescribe declaraciones escritas y firmadas en todas las circunstancias que requieran un consentimiento explícito. Por ejemplo, en el contexto digital o en línea, un interesado puede emitir la declaración requerida rellenando un impreso electrónico, enviando un correo electrónico, cargando un documento escaneado con su firma o utilizando una firma electrónica[420]. Por tanto, debemos colegir que el consentimiento, explícito no es sinónimo de consentimiento escrito[421].

En relación con lo anterior, debemos recordar que el consentimiento explícito en materia de protección de datos ha sido el escrito, en papel o en soporte electrónico; pero lo cierto es que la forma válida para consentir también puede ser verbal. El uso de declaraciones verbales puede ser una forma lo suficientemente manifiesta de expresar el consentimiento explícito. Sin embargo, este consentimiento verbal no resulta operativo porque puede resultar difícil para el responsable del tratamiento demostrar que se cumplieron todas las condiciones para el consentimiento explícito válido cuando se grabó la declaración. Existen no obstante algunas excepciones. Por ejemplo, se puede obtener el consentimiento explícito mediante una conversación telefónica, siempre que la información sobre las opciones del interesado sea inteligible y clara y se pida una confirmación específica del interesado, por ejemplo, pulsando un botón o proporcionando confirmación verbal.

---

[418] IBERLEY., "Consentimiento explícito en el Reglamento General de Protección de Datos (RGPD) y en la LO 3/2018 (LOPDGDD)", *iberley*, 30 de enero de 2019, disponible en: https://www.iberley.es/temas/consentimiento-explicito-materia-proteccion-datos-62819#:~:text=El%20t%C3%A9rmino%20expl%C3%ADcito%20se%20refiere,una%20declaraci%C3%B3n%20expresa%20de%20consentimiento *[Última consulta: 15 de junio de 2021]*

[419] CARVALHO, A. C.; MARTINS, R. y ANTUNES, L., "How-to express explicit and auditable consent", *IEEE*, 2018, p. 2, disponible en: 10.1109/PST.2018.8514204

[420] CEPD. Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 (WP 259), 4 de mayo de 2020, p. 20

[421] APARICIO SALOM, J. y VIDAL LASO, M., *Estudio sobre la protección de datos, cit.*, p. 150

Además del consentimiento verbal, existe otros métodos de consentimiento, por ejemplo, un paciente de un determinado centro sanitario puede recibir un correo electrónico por parte del responsable del tratamiento notificándole la intención de tratar determinados datos relativos a la salud suyos con un fin específico; si el interesado autoriza el uso de esos datos, el responsable le pedirá que envíe un correo electrónico de respuesta que contenga las palabras "estoy de acuerdo". Tras enviar su respuesta, el interesado recibirá un enlace de verificación en el que debe hacer clic o un mensaje SMS con un código de verificación para confirmar su autorización[422].

4.4. Carga de la prueba del otorgamiento del consentimiento:

Recuérdese que, cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales[423]. Si el responsable del tratamiento de los datos personales no es capaz de demostrar que el interesado otorgó el consentimiento, el tratamiento que haya efectuado se considerará ilícito en base al artículo 6.1. RGPD, infracción tipificada como muy grave en el artículo 72.1.b) LOPDGDD[424].

Pues bien, uno de los principales problemas a los que se enfrenta el responsable del tratamiento consiste en la obtención y conservación de medios de prueba que permitan acreditar que se ha obtenido el consentimiento por parte del interesado. Así, la carga de la prueba del otorgamiento del consentimiento tiene una relación directa con el punto anterior relativo al requisito de que el consentimiento sea inequívoco.

El RGPD no establece un mecanismo en concreto por el cual el responsable deba probar que ha obtenido un consentimiento válido, sino que este tiene libertad para implementar la forma de obtención y registro que más se adapte a los procesos de la organización. No obstante, el Reglamento exige que el responsable debe poder acreditar quién otorgó el consentimiento, cuándo, cómo y para qué, así como la información que se le suministró en el momento de obtenerlo. La obligación de demostrar que existe el consentimiento válido que legitima el tratamiento subsistirá mientras dure la actividad de tratamiento de los datos en cuestión. Una vez finalizada dicha actividad, la prueba del consentimiento no deberá conservarse más allá de lo estrictamente necesario para cumplir una obligación legal o para la formulación, el ejercicio o la defensa de reclamaciones. Como se ha dicho, si el fin de las operaciones de tratamiento cambian o evolucionan de manera considerable, el consentimiento original dejará de tener validez. En este caso, deberá obtenerse un nuevo consentimiento[425].

---

[422] Ibid., pp. 21-22

[423] Considerando 42 y artículo 7.1 del RGPD

[424] Véanse al respecto: Procedimientos sancionadores de la AEPD PS/00235/2019 de 21 de febrero de 2020, PS/00270/2019 de 24 de enero de 2020; PS/00405/2019 de 8 de enero de 2019 y PS/00025/2019 de 23 de diciembre de 2019

[425] CEPD., Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, *cit.*, p. 22

En el caso de que el consentimiento deba darse por escrito, el responsable del tratamiento debe conservar dicho documento para poder demostrar la existencia del consentimiento. De la misma manera, pueden utilizarse sistemas de documentación alternativos, como las grabaciones de imágenes o de sonido de la prestación del consentimiento[426]. El valor de esa grabación es idéntico a la conservación por el destinatario de una carta recibida por correo y su aportación a algún procedimiento como medio de prueba de las manifestaciones que se hacen en ella por parte del remitente, por lo que debe entenderse que dicha grabación es lícita. En el caso del comercio electrónico y relaciones por medio de Internet, si no existen tratos por medio de correo electrónico, la vía de acreditar que se ha consentido expresamente el tratamiento o la cesión de datos personales es la acreditación de la mecánica de funcionamiento de la página principal a través de la que se accede a la relación[427].

4.5. Revocación del consentimiento:

Cuando la base jurídica que legitima el tratamiento sea el consentimiento, el interesado tiene derecho a retirarlo o revocarlo en cualquier momento sin que el responsable del tratamiento pueda imponer condiciones gravosas que impidan o dificulten tal revocación[428]. Según el RGPD, el interesado tiene derecho a retirar su consentimiento en cualquier momento, debiendo ser informado de esta posibilidad antes de que otorgue el consentimiento[429]. La retirada no afecta a la licitud del tratamiento basada en el consentimiento previo. Esto es, la retirada del consentimiento no tiene efectos retroactivos, y por tanto el tratamiento que se realizó antes de la retirada del consentimiento será legítimo. A diferencia de la derogada LOPD[430], la actual normativa no exige que se justifique la causa del consentimiento. Es más, el RGPD refuerza dicha libertad al incorporar la frase "en cualquier momento".

---

[426] Actualmente la iniciativa "Kantara" (alianza, sin ánimo de lucro, que reúne a varias de las compañías mundiales que trabaja en mejorar el uso confiable de la identidad y los datos personales a través de la innovación, la estandarización y las buenas prácticas en el dominio de la gestión de la identidad digital y la privacidad de los datos) trabaja en la creación de un recibo del consentimiento, denominado "*Consent Receipt 1.0 (CR 1.0)*". Esta iniciativa pretende desarrollar un estándar de protección de datos que permita registrar el consentimiento en un formato común, estructurado, abierto e interoperable, basado en los códigos y buenas prácticas de la industria, que sirva para proporcionar al interesado un "recibo" de los tratamientos en los que consiente y le permita poder ejercer fácilmente sus derechos: rastrear los consentimientos prestados, conocer cómo se procesó su información o saber a quién responsabilizar en el caso de una brecha de seguridad. Esta herramienta permitiría a los interesados disponer de una forma de controlar y gestionar su consentimiento antes, durante y después del tratamiento haciéndoles realmente propietarios de sus datos personales, y a los responsables fomentar la transparencia y contar con un mecanismo de registro de consentimientos verificables. Véase al respecto: AEPD., "Recibo del consentimiento: Una herramienta de transparencia y responsabilidad proactiva", *aepd*, 27 de febrero de 2020, disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/recibo-del-consentimiento-una-herramienta-de-transparencia-y *[Última consulta: 17 de junio de 2021]*

[427] APARICIO SALOM, J. y VIDAL LASO, M., *Estudio sobre la protección de datos, cit.*, pp. 152-155

[428] IBERLEY., "Condiciones del consentimiento en materia de protección de datos en el Reglamento General de Protección de Datos (RGPD) y en la LO 3/2018 (LOPDGDD)", *cit.*

[429] Artículo 7.3 del RGPD

[430] Artículo 6.3 de la LOPD *"El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos."*

Retirar el consentimiento ha de ser tan fácil como otorgarlo[431]. Si el consentimiento es otorgado por medios electrónicos mediante un "clic" o deslizando el dedo por una pantalla, los interesados deben poder retirar su consentimiento de la misma manera. Cuando el consentimiento se otorgue mediante el uso de una interfaz de usuario específica de algún servicio como una aplicación, una cuenta de inicio o por correo electrónico, el interesado debe poder retirar el consentimiento a través de la misma interfaz electrónica, ya que cambiar a otra interfaz con el único fin de retirar el consentimiento requeriría un esfuerzo injustificado. Por ejemplo, si el interesado autorizó el tratamiento de sus datos personales mediante un "clic", no se le puede exigir que llame telefónicamente en un determinado horario de oficina para retirar el consentimiento, puesto que ésta última opción no es comparable a hacer un "clic"[432]. En todo caso, la retirada del consentimiento ha de ser gratuita, los medios de pago como las llamadas a números no gratuitos son inválidos[433].

Asimismo, el interesado debe poder retirar su consentimiento sin temor a sufrir perjuicio alguno. Esto significa que el responsable debe hacer posible la retirada de consentimiento de manera gratuita y sin que disminuya el nivel en la prestación del servicio.

5. EL PRINCIPIO DE TRANSPARENCIA COMO REQUISITO PARA REFORZAR EL CONSENTIMIENTO DEL INTERESADO:

Como se viene exponiendo, el RGPD otorga un valor especial al derecho a la información y al principio de transparencia con el fin de reforzar la figura del consentimiento del interesado. Esto es, el legislador ha identificado al presente requisito como un instrumento idóneo para reforzar la figura del consentimiento del interesado. No obstante, existen dudas en relación a la distinción entre ambos conceptos y su ámbito objetivo de aplicación. En un epígrafe anterior nos hemos referido de forma somera al principio de información del interesado, recuperamos aquí el hilo de dicho análisis para distinguirlo del principio de transparencia incorporado a la normativa europea mediante el RGPD.

5.1. El principio de transparencia como un concepto distinto de la información debida al interesado:

Como se ha dicho en reiteradas ocasiones, el derecho fundamental a la protección de datos otorga al interesado un poder de disposición y control sobre los datos personales, le permite saber quién posee esos datos personales y para qué, pudiendo oponerse a esa

[431] Artículo 7.3 del RGPD
[432] CEPD., Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, *cit.*, p.23
[433] ANDRÉS RICART, G., "El consentimiento y el Reglamento de Protección de datos", *legaltoday*, 4 de octubre de 2019, disponible en: https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/el-consentimiento-y-el-reglamento-de-proteccion-de-datos-2019-10-04/ *[Última consulta: 20 de junio de 2021]*

posesión o uso. Sin embargo, el interesado no podrá ejercer dicho derecho si desconoce, entre otras cuestiones, el fin que justifica el tratamiento de sus datos personales, quién es el responsable del tratamiento y que derechos tiene.

Recuérdese que el Tribunal Constitucional en su sentencia 292/2000, de 30 de noviembre, declaró que el principio de información forma parte del contenido esencial del derecho fundamental a la protección de datos personales. Gracias a este derecho, el interesado adquiere un conocimiento que le permite ejercer un control sobre sus datos personales, de manera que puede otorgar el consentimiento para el tratamiento de sus datos o ejercitar sus derechos. Siguiendo esta misma línea, SÁNCHEZ CARAZO ha afirmado que el derecho a la información es un derecho raíz, puesto que sin la información no se pueden ejercer el resto de los derechos. Para poder consentir sobre cómo se tratan los datos, se ha de tener una información clara y veraz; si no se tiene información no se puede consentir y si no se está bien informado ni se pueden tomar decisiones, ni se puede ejercer la autonomía ni la libertad[434].

Lo mismo se predica del ejercicio de los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición o la posibilidad de revocar que no podrán ser ejercitados si el interesado carece de información sobre el tratamiento de sus datos. La clave para la protección de datos es que el interesado esté informado acerca de todas las circunstancias que concurren en el tratamiento, a efectos de que pueda prestar su consentimiento y que lo mantenga porque el tratamiento en cuestión no vulnera sus intereses particulares[435]. La información junto con los otros tres requisitos del consentimiento no solo hace que el consentimiento sea válido, sino que además tienen la función de facilitar el ejercicio de los derechos del interesado.

El artículo 6.a) de la Directiva derogada disponía que los datos personales debían ser tratados de manera leal y lícita. Como novedad, el artículo 5.a) del RGPD prevé que los datos personales serán tratados de manera lícita, leal y transparente. Así, el RGPD contempla un nuevo principio del tratamiento de los datos personales en el citado artículo[436], desarrollado en el artículo 12 del mismo cuerpo legal[437].

Se ha dicho que el principio de transparencia se refiere tanto al deber que tiene el responsable de informar al interesado acerca de ciertos elementos del tratamiento de sus datos personales como a la manera en que se cumple dicha obligación[438]. En este

---

[434] SÁNCHEZ CARAZO, C., "La protección de datos personales de las personas vulnerables", *Anuario de la Facultad de Derecho de la Universidad de Alcalá II*, Núm. 2, 2009, p. 203

[435] APARICIO SALOM, J. y VIDAL LASO, M., *Estudio sobre la protección de datos, cit.*, p. 167

[436] HERNÁNDEZ CORCHETE, J.A. "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos", en PIÑAR MAÑAS, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo de Privacidad*, Reus, Madrid, 2016, p. 206

[437] Artículo 12 del RGPD: "*en forma concisa,* ***transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo****, en particular cualquier información dirigida específicamente a un niño".*

[438] Considerando 58 del RGPD: *"El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la*

sentido, el Considerando 39 del RGPD explica que el principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Se refiere en particular al deber de facilitar la información relativa a la identidad del responsable del tratamiento y a los fines del mismo, así como a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. En definitiva, la transparencia obliga a informar al interesado sobre el tratamiento de sus datos personales de una manera, pero también implica una prohibición: la de llevar a cabo cualquier otro tratamiento que no conozca el interesado[439]. En este sentido, La LOPDGDD recoge en su preámbulo que, el Título III dedicado a los derechos de las personas adapta al Derecho español el principio de transparencia del reglamento europeo, que regula el derecho de los afectados a ser informados acerca del tratamiento y recoge la denominada "información por capas" como modo en el que se debe presentar la información. Por tanto, si el responsable no proporciona información accesible, el control del usuario será ilusorio y el consentimiento no constituirá una base válida para el tratamiento de los datos[440].

El legislador afirma que, por ejemplo, en el ámbito tecnológico, el simple cumplimiento de informar al interesado no garantiza de un modo efectivo que este sea consciente de la lógica a que obedece el tratamiento de sus datos personales, de modo que aumenta su sensación de no tener un poder efectivo de disposición sobre sus datos. Esta situación es la que se pretende solucionar imponiendo que la información indicadas en los artículos 13 y 14 del RGPD, así como cualquier comunicación con arreglo a los artículos 15-22 y 34 del RGPD se realicen conforme a un deber de transparencia[441].

Por otra parte, el RGPD exige que el principio de transparencia ha de estar presente durante todo el tratamiento de los datos, y no solo a la hora de proporcionar la información al interesado. Puesto que, en el artículo 5.1 del RGPD se recoge que los

---

práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender".

[439] STJUE (Sala Segunda), de 11 de noviembre de 2020, Orange Romania, C-61/19, ECLI:EU:C:2020:901, apartado 40: "*el responsable del tratamiento facilitará al interesado información respecto de todas las circunstancias relacionadas con el tratamiento de datos, con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, debiendo el interesado conocer, en particular, qué datos serán tratados, la identidad del responsable del tratamiento, la duración del tratamiento y su forma, y los fines que se persigue con dicho tratamiento. Esta información debe permitir a esa persona determinar fácilmente las consecuencias de cualquier consentimiento que pueda dar y garantizar que dicho consentimiento se otorgue con pleno conocimiento de causa";* y STJUE (Gran Sala), de 1 de octubre de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801, apartado 74: *"una información clara y completa debe permitir al usuario determinar fácilmente las consecuencias de cualquier consentimiento que pueda dar y garantizar que dicho consentimiento se otorgue con pleno conocimiento de causa".*

[440] CEPD. Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, *cit.*, p. 5

[441] HERNÁNDEZ CORCHETE, J.A. "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos", *cit.*, p. 207

datos personales serán tratados de manera lícita, leal y transparente. El responsable del tratamiento debe cumplir el principio de transparencia tanto a la hora de informar al interesado como en el transcurso del tratamiento de los datos personales. De esta forma, atendiendo al momento en que debe hacerse efectivo el deber de transparencia por parte del responsable o del encargado, han de diferenciarse por una parte, el momento en que el responsable asume la capacidad de decisión sobre los datos de la persona, en el que nace la obligación de informar acerca de las características del tratamiento que tiene intención de realizar (deber de información); y por otra, el supuesto sobrevenido de obligación de transparencia, que exige informar al interesado acerca de las nuevas circunstancias tan pronto como se produce un cambio sustancial en el tratamiento[442].

5.2. Sujetos obligados a informar:

El GT29 puso de relieve que este deber de informar incumbe al responsable del tratamiento al afirmar que las disposiciones relativas a los derechos de los interesados a la información han sido formuladas de tal manera que implican la creación de obligaciones para el responsable del tratamiento[443]. Esta obligación no ha de entenderse solamente como un deber del responsable o encargado del tratamiento, puesto que el incumplimiento de dicha obligación privaría al interesado de un derecho que posee.

Respecto al receptor de la información, este ha de ser el interesado. Esto es, el responsable del tratamiento debe dirigirse al interesado para cumplir con su obligación de informar. A modo de ejemplo, en el caso de los hospitales, como norma general el responsable del tratamiento será el mismo centro sanitario, y el paciente en cuestión será el interesado.

5.3. Contenido de la información que el responsable del tratamiento ha de facilitar al interesado:

El RGPD recoge en los artículos 13 y 14 la información que el responsable del tratamiento deberá facilitar al interesado. Este contenido varía si los datos personales han sido obtenidos del interesado o no. En el primer caso, el responsable del tratamiento deberá informar sobre los puntos recogidos en el artículo 13 del RGPD, y en el segundo caso, cuando los datos no se hayan obtenido del interesado, sobre los puntos recogidos en el artículo 14 del RGPD. Tal y como se ha señalado, esta distinción también afecta al momento en el que el responsable del tratamiento debe cumplir con su deber de información. Cuando los datos hayan sido recogidos directamente del interesado, el responsable deberá aportarle toda la información que se recoja en el artículo 13 del RGPD al tiempo de la recogida de los datos. Sin embargo, cuando los datos no se hayan

[442] APARICIO SALOM, J. y VIDAL LASO, M., *Estudio sobre la protección de datos*, *cit.*, p. 207

[443] GT29., Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», 00264/10/ES (WP 169), de 16 de febrero de 2010, p. 4; STJUE (Gran Sala), de 10 de julio de 2018, Jehovan todistajat, C–25/17, ECLI:EU:C:2018:551

obtenido del interesado, el responsable deberá otorgarle toda la información que se recoja en el artículo 14 del RGPD dentro de un periodo no superior a un mes.

Los dos artículos presentan la misma estructura: en su primer apartado ambos recogen un conjunto de datos que el responsable deberá de proporcionar al interesado, y en el segundo apartado, se refieren a la información que deberá proporcionarse para respetar los principios de transparencia y lealtad. Dentro del primer apartado, se recogen una serie de informaciones comunes debidas al interesado: la identidad y los datos de contacto del responsable y, en su caso, de su representante; los datos de contacto del delegado de protección de datos, en su caso; los fines del tratamiento; los destinatarios o las categorías de destinatarios de los datos personales; y, en su caso, la intención del responsable de transferir los datos personales a un tercer país u organización internacional. No obstante, aunque compartan los mencionados puntos, el artículo 13.d) se refiere a que, cuando el tratamiento se base en el artículo 6.1.f), se deberán especificar los intereses legítimos del responsable o de un tercero. Por su parte, el artículo 14.d) obliga a informar al interesado sobre las categorías de datos personales de que se trate.

Como se verá más adelante, las Autoridades de Protección de Datos se recomienda adoptar un modelo de información por capas o niveles a la hora de informar. Este enfoque consiste en presentar una información básica en un primer nivel y remitir a la información adicional en un segundo nivel donde se presentará detalladamente el resto de la información. En este sentido, el artículo 11.2 del LOPDGDD recoge que, dentro de la información contenida en el artículo 13.1 se considerará información básica la identidad del responsable del tratamiento, la finalidad del tratamiento y la posibilidad de ejercer los derechos establecidos en los artículos 15 a 22 del RGPD. Por su parte, el artículo 11.3 del LOPDGDD establece que, dentro de la información contenida en el artículo 14.1 se considerará información básica la respectiva a las categorías de datos objeto de tratamiento y las fuentes de las que procedieran los datos. Por tanto, el responsable del tratamiento deberá aportar, dependiendo si los datos se han recogido directamente del interesado o no, por lo menos la citada información en esta primera capa de información.

Además, en los artículos referidos exige que el responsable del tratamiento deberá informar sobre los siguientes extremos: el plazo durante el cual se conservarán los datos personales, y cuando lo anterior no sea posible, los criterios utilizados para determinar ese plazo; la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales, su rectificación o supresión, la limitación u oposición de su tratamiento, así como el derecho a la portabilidad de los datos; la existencia del derecho a retirar el consentimiento en cualquier momento; el derecho a presentar una reclamación ante una autoridad de control; y la existencia de decisiones automatizadas, incluida la elaboración de perfiles. Por su parte, el artículo 13.2.e) exige que se informe sobre si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales

datos. En cuanto al artículo 14.2, en el apartado b) se requiere que se informe sobre los intereses legítimos del responsable del tratamiento o de un tercero cuando el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, y en el apartado f) sobre la fuente de la proceden los datos personales y, en su caso, si proceden de fuentes de acceso público. La segunda capa contendrá toda esta información adicional. En el caso de que el responsable del tratamiento no informe sobre todos los puntos exigidos por la normativa referida incurrirá en una infracción grave[444].

5.4. Forma en la que ha de facilitarse la información:

La información puede presentarse de maneras distintas, por ejemplo, mediante declaraciones escritas, medios electrónicos o verbales[445]. Es más, la AEPD admitió que para el tratamiento de datos derivados del pago de productos o servicios mediante tarjeta de crédito u otro instrumento similar, no sería preciso que la cláusula informativa constase expresamente en el ticket de pago pudiendo acudirse a mecanismos alternativos que garantizasen el conocimiento por el interesado del tratamiento de sus datos, apuntándose la posibilidad de que se ubicase en cada punto de pago un cartel suficientemente visible y legible[446].

El artículo 12.7 del RGPD establece que la información que deberá facilitarse a los interesados podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. En cuanto a los iconos que se presenten en formato electrónico, serán legibles mecánicamente. La eficaz realización de la función que se asigna a los iconos depende de su sencillez y de que sean universalmente identificables[447]. Sin embargo, la información mediante iconos por sí sola no es suficiente para entender realizado el deber de informar, puesto que con la frase "en combinación" se entiende que los iconos han de ser un complemento de otros medios de informar, no la principal vía de información.

Ya se ha dicho que los responsables del tratamiento deben suministrar la información de una forma concisa y transparente. El responsable ha de utilizar frases breves y claras

[444] En este sentido el banco BBVA fue sancionado con una multa por importe de dos millos de euros por infringir el deber de informar al no especificar la categoría de datos que trataría, limitándose a advertir al interesado de forma genérica que podría tratar datos económicos y de solvencia patrimonial, datos transaccionales y datos sociodemográficos. A la vista de dicha información, no quedaba claro si el banco trataría datos económicos ajenos a los productos contratados con la entidad o comercializados por la misma, qué datos personales registraría por cada transacción o qué datos sociodemográfico trataría. Véase al respecto: AEPD resolución de procedimiento sancionador núm. PS/00070/2019 de 13 de enero de 2021

[445] Es posible facilitar la información verbalmente de manera automatizada además de por los medios escritos. Por ejemplo, esto puede aplicarse en el contexto de las personas con alguna discapacidad visual en su interacción con prestadores de servicios de la sociedad de la información, o en el contexto de dispositivos inteligentes sin pantalla. Véase al respecto: GT29. Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, 17/ES (WP260), de 11 de abril de 2018, p. 14

[446] AEPD informe jurídico núm. 0029/2011 de 14 de marzo de 2011

[447] HERNÁNDEZ CORCHETE, J.A. "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos", *cit.*, p. 213

para informar al interesado. De esta manera, se pretende evitar la fatiga informativa del interesado. Asimismo, esta información debe diferenciarse claramente de otra información no relacionada con la privacidad. Es errónea la idea de que cuanta más información se proporcione al interesado mejor comprenderá este su contenido. De ahí la importancia de la "información por capas" a la que nos referiremos más adelante.

El requisito de que la información sea inteligible se refiere a que debe resultar comprensible para el receptor. Los responsables del tratamiento deben asegurarse de que utilizan un lenguaje claro y sencillo en todos los casos[448], evitando oraciones y estructuras lingüísticas complejas. La información debe ser concreta y categórica, no debe formularse en términos abstractos o ambivalentes ni dejar margen para distintas interpretaciones. En concreto, los fines y la base jurídica del tratamiento de los datos personales deben ser claros[449]. Los responsables del tratamiento no pueden utilizar documento de políticas de privacidad muy extensas que sean difíciles de entender o declaraciones técnicas basadas en la jerga jurídica[450]. En este aspecto, el RGPD va más allá de lo que disponía el artículo 5 de la derogada LOPD, que tan solo exigía que la información se prestara de modo expreso, preciso e inequívoco. Será necesario que las cláusulas informativas expliquen el contenido de una forma clara y accesible para los interesados, con independencia de sus conocimientos en la materia[451].

Al tiempo que la capacidad de comprensión del interesado, ha de tenerse también en cuenta la accesibilidad de la información. La expresión "de fácil acceso" que se recoge en el artículo 12.1 del RGPD implica que el interesado debe poder reconocer inmediatamente dónde y cómo acceder a esta información, sin tener que realizar búsquedas complejas. Tanto el artículo 13.1 como el 14.1 del mismo cuerpo legal recogen que el responsable del tratamiento "facilitará toda la información". La palabra clave en esta expresión es "facilitará", puesto que se refiere a la obligación del responsable del tratamiento de adoptar medidas activas para suministrar la información[452]. El responsable del tratamiento debe valorar el tipo de público que proporciona datos a su organización a partir de dicha valoración debe reflexionar sobre cómo presentará dicha información a los interesados. Este requisito de accesibilidad cobra especial importancia en el caso de las personas mayores.

Por ejemplo, si una persona mayor quiere descargar una aplicación sanitaria, esta persona debe contar con información que pueda comprender fácilmente. Es necesario

---

[448] El RGPD hace especial referencia a la redacción de la política de protección de datos que deberán aceptar los menores de edad en su artículo 12.1 al introducir la oración "*en particular cualquier información dirigida específicamente a un niño*". Sin embargo, no menciona ningún otro colectivo al que debería de "ajustarle" el formato de la información proporcionada.

[449] GT29. Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, *cit.*, p. 9

[450] CEPD. Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, *cit.*, p. 15

[451] IBERLEY., "Derecho de transparencia e información en la LO 3/2018 (LOPDGDD) y en el Reglamento General de Protección de Datos (RGPD)", *iberley*, 18 de enero de 2019, disponible en: https://www.iberley.es/temas/derecho-transparencia-informacion-lopdgdd-rgpd-62754 *[Última consulta: 20 de junio de 2021]*

[452] GT29. Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, *cit.*, p. 20

que se le informe mediante un lenguaje claro y sencillo. Las frases han de ser cortas y se han de utilizar palabras de fácil comprensión. Igualmente, el tamaño de fuente de letra utilizado ha de ser adecuado para este tipo de usuario. En el caso de la aplicación debe aparecer una ventana emergente que contenga la información antes de que otorgue su consentimiento. Igualmente, esta información ha de estar siempre fácilmente localizable[453], siendo conveniente incluir un apartado permanente en el menú de la aplicación.

Como el responsable del tratamiento tiene la obligación de diferenciar la información para las actividades de tratamiento de datos personales y la información relativa a otras cuestiones, lo más adecuado sería que la hoja informativa que contiene tanto la información básica como la adicional estuviese separada físicamente de la hoja informativa "clínica" que contiene la información del tratamiento sanitario, aunque como se ha dicho más arriba esto no es estrictamente necesario. Si toda la información se encuentra mezclada y en un único documento será difícil que interesado pueda comprender completamente todo el contenido del mismo.

5.4.1. Información por capas:

Con el fin de hacer compatible la obligación de informar y la concisión y comprensión en la forma de presentarla, las Autoridades de Protección de Datos se recomienda adoptar un modelo de información por capas[454] o por niveles. La información multinivel consiste en presentar una información básica en un primer nivel, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos, y remitir el resto de las informaciones a un segundo nivel donde se presentarán más detalladamente. Este enfoque pretende facilitar la tarea del responsable del tratamiento a la hora de diseñar sus procedimientos y formularios, y además, procura que las personas interesadas obtengan la información más relevante de forma rápida y simplificada[455].

El enfoque de doble capa informativa es útil ya que permite proporcionar información clave de privacidad de inmediato y tener información más detallada disponible en otros lugares[456]. El responsable tiene el deber de otorgar la información, pero si no lo hace de forma concisa, transparente, inteligible, utilizando un lenguaje claro y sencillo y poniéndolo accesible para el interesado, estará infringiendo la normativa de protección de datos. Gracias a la estructura de capas, se consigue que el interesado no sea abrumado con la información, y que pueda comprenderla adecuadamente.

---

[453] La información, en forma de política de privacidad, debe estar disponible tanto en la propia aplicación como en la tienda de aplicaciones. De esta forma, el usuario podrá consultarla antes de instalar la aplicación o en cualquier momento durante su uso. Véase al respecto: AEPD., "El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles", *cit.*, p. 1

[454] AEPD. Informe jurídico núm. 210070/2018 de 19 de diciembre de 2018

[455] AEPD. Guía para el cumplimiento del deber de informar, 25 de mayo de 2018, p. 5

[456] GONZÁLEZ, Y., "La información por capas en el RGPD", *grupoatico34*, 27 de marzo de 2020, disponible en: https://protecciondatos-lopd.com/empresas/informacion-por-capas-rgpd/ *[Última consulta: 22 de junio de 2021]*

En concreto, según indica la AEPD, en cuanto a la primera capa, debe estar identificada con un título tal como "información básica sobre protección de datos", y la forma de presentación preferente es en forma de tabla, garantizando que dicha información quede dentro del "campo de visión" del interesado, según sea el medio utilizado en la recogida de la información. Dentro de la tabla se han de recoger los siguientes cinco epígrafes: "responsable", "finalidad", "legitimación", "destinatarios" y "derechos". A estos cinco epígrafes se les añadirá un sexto, el de la "procedencia" cuando los datos no procedan del propio interesado.

Por ejemplo, en un formulario de solicitud, la tabla con la información básica debería situarse en el mismo campo de visión que el lugar donde haya de manifestarse la conformidad con lo solicitado (la firma, si es en papel, o el botón de "enviar", si es un formulario electrónico), formando parte de la copia que quede a disposición del interesado. Si por restricciones del diseño no fuese factible, debe incorporarse una nota o llamada en el campo de visión de la firma informando sobre dónde se sitúa la tabla con la información sobre protección de datos[457]. El mismo "formato tabla" hace que la información que se incorpore a la misma no sea extensa y que se identifique cada punto fácilmente. Su función es informar sobre los elementos indispensables clara y brevemente.

Respecto a la segunda capa, esta desarrolla los puntos de la primera y añade información adicional. Así, en el primer epígrafe, el del responsable, se debe completar su información incorporando los siguientes datos: identidad y datos de contacto del responsable, datos de contacto del Delegado de Protección de Datos (dirección postal y dirección electrónica si se dispone). Seguidamente, en el epígrafe de la finalidad, se describirá con mayor detalle los fines del tratamiento al que se destinan los datos personales, incluyendo el plazo durante el cual se conservarán dichos datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo. En su caso, dentro del segundo epígrafe, se informará de la existencia de decisiones automatizadas, incluida la elaboración de perfiles. Respecto al epígrafe de la legitimación, se desarrollará la base jurídica en la cual se basa el tratamiento. Es decir, en la información básica se ha de decir la base jurídica del tratamiento, y en la información adicional se desarrollará dicha base jurídica con más detalle.

Cuando se haya previsto ceder los datos personales, se informará al interesado sobre la identidad de los destinatarios, si están claramente predeterminados, o de las categorías de destinatarios, si estos no están determinados previamente. También es conveniente informar de la existencia de encargados de tratamiento, cuya legitimidad del tratamiento es la ejecución del contrato del encargo. Cuando se haya previsto transferir datos personales a un tercer país u organización internacional, se deberá informar a los interesados de las condiciones que afectan a dicha transferencia. En el epígrafe de los derechos, se explicará el contenido de cada uno de los derechos que tiene el interesado y cómo puede ejercerlos. Igualmente, el interesado deberá de informarle sobre la

[457] Ibíd., p. 6

posibilidad de presentar una reclamación ante Autoridad de Control en materia de Protección de Datos competente. Dado que este epígrafe es uno de los que contiene mayor información, se ha de mantener en todo momento un lenguaje claro y sencillo, siempre con frases cortas y comprensibles. Por último, en el caso de que los datos personales no hayan sido obtenidos por el interesado (por proceder de alguna cesión legítima, o de fuentes de acceso público), se incorporará un último epígrafe, el de la procedencia, debiendo informar sobre la categoría de los datos personales y la fuente de la que proceden.

Es claro, por otra parte, que puede proporcionarse voluntariamente información no requerida por el RGPD, siempre que contribuya a una mejor transparencia y lealtad del tratamiento. Aunque en esta segunda capa se amplíe la información, no debe dejarse a un lado el requisito de informar clara y sencillamente. La información se puede facilitar en una tabla o de otro modo. En este segundo caso, se ha de utilizar una exposición bien estructurada, por ejemplo, en base a preguntas y respuestas, siguiendo los epígrafes generales antes descritos[458].

En cuanto al medio, las capas pueden consistir en un formato físico, electrónico o telefónico. Así, la información adicional puede estar contenida, por ejemplo, en el reverso del documento que contiene la tabla, en un documento separado que se entregue al interesado y que pueda este pueda conservar. Pero, la información adicional también puede recogerse en una página web específica, incorporando, por ejemplo, el enlace a la misma en la tabla inicial. Por último, respecto al formato telefónico, se tratará de una locución accesible electrónicamente o remitida, por correo postal o electrónico. Aunque la normativa permita estas tres vías de otorgar la información adicional, cuando el público al que va dirigido esta información sea mayor, la vía más adecuada sería la del formato físico. En suma, la información por capas consiste en dividir la información facilitada a los usuarios en una primera capa más genérica y una segunda capa más detallada.

5.4.2. La información debida al interesado/receptor de edad avanzada:

Como se viene exponiendo, para que el consentimiento sea válido, ha de ser libre, específico, informado e inequívoco. Tienen que cumplirse los cuatro requisitos. Pero existen ciertos elementos que afectan igualmente la validez del consentimiento y están unidos a los citados cuatro requisitos, por ejemplo, la capacidad, el nivel cultural y la situación personal del interesado. Así, las limitaciones cognitivas junto con el perfil demográfico y cultural de los interesados, afectan e influyen en el complejo proceso de otorgar el consentimiento[459]. En relación directa con el modo en el que el responsable

[458] APDCAT, Guía para el cumplimiento del deber de informar en el RGPD, *cit.*, p. 13
MITTAL, S. y SHARMA, P., "The role of consent in legitimising the processing of personal data under the current EU data protection framework", *Asian Journal of Computer Science And Information Technology*, *cit.*, p. 77

del tratamiento ha de cumplir con su deber de información[460], debemos hacer referencia al fenómeno de la brecha digital a la que se enfrenten a menudo las personas mayores. La llamada brecha digital es la distancia que se abre entre las personas con acceso y conocimiento eficiente de las TIC y las que no. Esta brecha se intensifica a través de las diferencias socioeconómicas, edad y nivel educativo[461].

En referencia al citado fenómeno, PRENSKY sitúa a dos grupos en cada extremo de la brecha: los "nativos digitales" y "los inmigrantes digitales". El primer grupo, también conocidos como "*millenials*", "generación net" o "generación digital", se refiere al grupo de personas que prácticamente han nacido rodeados de tecnología, encontrándose totalmente familiarizados con la misma. En el segundo grupo, "los inmigrantes digitales", son aquellos que no nacieron "en el mundo digital". Las personas mayores deben aprender el idioma de la nueva tecnología. Dejando a un lado la discusión sobre la adecuación de los términos utilizados por el autor, queda patente que la sociedad está dividida en dos mitades: los que saben utilizar la tecnología y los que no[462].

Según una encuesta sobre el equipamiento y uso de Tecnologías de la Información y Comunicación en los hogares realizada por el Instituto Nacional de Estadística, la edad es un factor importante en el uso de las nuevas tecnologías. Las personas entre 16 y 24 años son las que más utilizan estas nuevas tecnologías, habiendo utilizado internet el 99,8% de ellos en los últimos tres meses. Este porcentaje va descendiendo conforme aumenta la edad. A partir de los 55 años se sitúa en el 89,5% y en el grupo de 65 a 74 años baja hasta el 69,7%. Respecto a los dispositivos o servicios de domótica, la mayor utilización se da en el grupo de 25 a 34 años, con un 37,9%. En cambio, el 87,2% de las personas entre 65 y 74 años no utiliza ninguno de estos dispositivos[463]. El reciente auge y desarrollo de las nuevas tecnologías no ha permitido un continuo contacto con este colectivo; además, se sienten ajenas a la tecnología o no se encuentran cómodas ni preparadas ante ella, ya que no han recibido una formación adecuada. En muchas ocasiones se genera incluso desconfianza. En otras ocasiones, el propio servicio que ofrecen el conjunto de las nuevas tecnologías no está enfocado ni aplicado a los posibles usos concretos útiles para las personas de determinada edad[464].

La brecha digital no se refiere únicamente al acceso a las nuevas tecnologías, lo que supondría la primera brecha digital, sino que también se refiere a la falta de

[460] SCHERMER, B.W.; CUSTERS, B.; VAN DER HOF, S., "The crisis of consent: How stronger legal protection may lead to weaker consent in data protection", *cit.*, p. 172
[461] MACÍAS GONZÁLEZ, L. y MANRESA YEE, C., "Mayores y nuevas tecnologías: motivaciones y dificultades", *Ariadna: cultura, educación y tecnología*, Vol. 1, Núm. 1, 2013, p. 7
[462] PRENSKY, M., "Digital natives, digital immigrants. On the horizon", *MCB university press*, Vol. 9, Núm. 5, 2001, pp. 1-2
[463] INE., "Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares Año 2020", *ine*, 16 de noviembre de 2020, disponible en: https://www.ine.es/prensa/tich_2020.pdf
[464] GONZÁLEZ OÑATE, C. y FANJUL PEYRÓ, C., "Aplicaciones móviles para personas mayores: un estudio sobre su estrategia actual", *cit.*, p. 109

alfabetización digital, siendo esta última la segunda brecha digital[465]. Es decir, el problema no se encuentra simplemente en el acceso condicionado a la base tecnológica[466] (disponer de banda ancha, ordenador, móvil…), sino que se extiende al hecho de saber utilizar las herramientas digitales[467].

La brecha, como metáfora, representa una grieta, una separación de dos mitades que teóricamente deberían estar unidas y al mismo nivel. Adquiere un carácter de ruptura en diversas dimensiones, que es precisamente aquello que trata de evitar o subsanar la alfabetización digital[468]. Por tanto, es necesario fomentar acciones formativas dirigidas al desarrollo de habilidades técnicas, sociales y éticas relativas al uso de las TIC de las personas adultas. Es cierto que con el tiempo este problema se irá solventando, a medida que las generaciones alfabetizadas digitalmente lleguen a la edad avanzada, pero hasta que eso sea una realidad, es necesario fomentar las acciones formativas dirigidas a este sector poblacional con metodologías adaptadas a sus necesidades, capacidades y limitaciones[469]. Para ello, el Gobierno junto con las comunidades autónomas deberá tener en especial consideración a las personas mayores en su Plan de Acceso a Internet[470]. El eje vertebrador de la inclusión de las personas mayores en la sociedad digital en condiciones de igualdad sustantiva, real y efectiva al resto de los ciudadanos, se ha de asentar sobre los irrenunciables criterios vectores de alfabetización digital,

---

[465] En este sentido se refiere el Grupo de Trabajo sobre Derechos Digitales de los Ciudadanos: "*La brecha digital entre países, o entre territorios dentro de un mismo país, crea asimetrías, impide una participación activa y global y aumenta aún más la brecha entre países ricos y pobres. Por eso es necesario un mayor grado de alfabetización digital de las personas, con mayor eficiencia y uso eficaz de los recursos disponibles. Es necesario, por tanto, romper las barreras económicas, técnicas, sociales y en su caso regulatorias para reducir la desigualdad y la pobreza. Eso significa, por un lado, facilitar el despliegue de las infraestructuras necesarias y, por otro, fomentar la capacitación digital de los ciudadanos".* GRUPO DE TRABAJO SOBRE DERECHOS DIGITALES DE LOS CIUDADANOS., "Primer conversatorio de derechos digitales de los ciudadanos", *red*, 31 de mayo de 2017, disponible en: https://www.red.es/redes/es/magazin-red/reportajes/el-primer-conversatorio-sobre-los-derechos-digitales-sit%C3%BAa-espa%C3%B1a-la *[Última consulta: 24 de junio de 2021]*

[466] El derecho al acceso universal a Internet está recogido en el artículo 81 de la LOPDGDD. El Estado debe garantizar que todos tengan este derecho con independencia de su condición personal, social, económica o geográfica. Además este acceso debe ser universal, asequible, de calidad y no discriminatorio para toda la población. Asimismo, se debe atender a la realidad específica de los entornos rurales y garantizar condiciones de igualdad para las personas que cuenten con necesidades especiales en sus conexiones a Internet. Respecto al derecho a la educación digital, recogido en el artículo 83 del mismo cuerpo legal, simplemente habla de los alumnos, no amparando el caso de las personas mayores.

[467] ABAD ALCALÁ, L., "Diseño de programas de e-inclusión para alfabetización mediática de personas mayores Comunicar", *Revista científica iberoamericana de comunicación y educación*, Núm. 42, 2014, p. 179

[468] MORENO RODRÍGUEZ, M.D., "Alfabetización digital: el pleno dominio del lápiz y el ratón", *Comunicar*, Vol. 15, Núm. 30, 2008, p. 140

[469] En un estudio realizado en Francia, Reino Unido y España se concluyó que la población de mayores en España es la que más baja adaptación tiene en relación a uso de las nuevas tecnologías y que, principalmente, este suceso viene determinado por la escasa formación y educación que las personas mayores tienen en el campo de las TIC. Estos resultados invitan a la puesta en marcha de nuevas iniciativas dirigidas a este colectivo de una manera más específica y con metodologías adaptadas a sus necesidades, capacidades y limitaciones. Véase al respecto: GONZÁLEZ OÑATE, C.; FANJUL PEYRÓ, C. y CABEZUELO LORENZO, F., "Uso consumo y conocimiento de las nuevas tecnologías en personas mayores en Francia, Reino Unido y España", *Comunicar*, Núm.45, 2015, p. 27

[470] El Plan de Acceso a Internet se recoge en el artículo 97 de la LOPDGDD dentro de las políticas de impulso de los derechos digitales.

confianza, seguridad y respeto de sus derechos fundamentales, destacando su derecho a la protección de datos[471].

La alfabetización digital debe representar la adquisición de los recursos intelectuales necesarios para interactuar tanto con la cultura existente como para recrearla de un modo crítico y emancipador y, en consecuencia, como un derecho y una necesidad de los ciudadanos de la sociedad informacional[472]. Por tanto, se ha revolucionado el concepto tradicional de la alfabetización. Dado que la presencia de estas nuevas tecnologías es cada vez más notoria en nuestro día a día, las personas mayores han de adquirir estos nuevos conocimientos. Se ha de "realfabetizar" a lo alfabetizados[473].

Por otra parte, la información que se les otorga a las personas mayores para el tratamiento de sus datos personales ha de ser lo más clara y sencilla posible[474]. A su vez, como sabemos, cuando existen diversos tratamientos posibles, el interesado deberá consentir o denegar por separado cada uno de ellos. Pero este otorgamiento del consentimiento por separado no se realizará con todas las garantías si el interesado no puede comprender el alcance de cada uno de dichos tratamientos.

Por ello, la información que se facilite a las personas mayores ha de ser fácilmente accesible y claramente visible (ubicación y tamaño de los caracteres…), debiendo utilizarse un lenguaje sencillo, claro y adaptado a la realidad sociocultural de sus destinatarios, así como complementarse el texto con imágenes o gráficos cuando ello facilite la comprensión del mismo. Igualmente, teniendo en cuenta el desfase generacional que separa a las personas mayores respecto de las nuevas tecnologías, cobra especial importancia determinar cómo se informará sobre la recogida y uso de sus datos personales[475].

5.5. Excepciones a la obligación de facilitar información:

Como norma general, el responsable del tratamiento tiene la obligación de informar al interesado, no obstante, en base a los artículos 13.4 y 14.5 del RGPD, esta obligación

[471] GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M., "La proteccion de datos de las personas mayores, necesidad y reto para una innovación tecnológica de calidad", en VALERO TORRIJOS, J., *La protección de los datos personales en Internet ante la innovación tecnológica: riesgos, amenzadas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, p.571

[472] AREA MOREIRA, M., "La alfabetización digital y la formación de la ciudadanía del siglo XXI", *Revista Integra Educativa*, Vol. 7, Núm. 3, 2014, p. 4

[473] GUTIERREZ MARTÍN, A., *Alfetización digital algo más que ratones y teclas*, Gedisa, Barcelona, 2003, p. 71

[474] A diferencia de la información proporcionada a los mayores, la normativa hace una especial referencia al caso de los menores. En este mismo sentido, la AEPD en su informe jurídico núm. 0046/2010 de 6 de abril de 2010 afirmaba que la obligación de informar exige un mayor rigor cuando el consentimiento se obtiene de un menor de edad, puesto que se dirige a una persona todavía no formada.

[475] GÓMEZ-JUAREZ SIDERA, I., "Hacia un nuevo derecho de protección de datos para las personas especialmente vulnerables en la sociedad digital del siglo XXI: los niños y las personas mayores", *Revista CESCO de Derecho de Consumo*, Núm. 4,2015, p. 238

tiene ciertas excepciones[476]. Todas las excepciones deberán poder ser justificadas por el responsable del tratamiento para acreditar por qué no ha cumplido con su deber de informar.

En primer lugar, el RGPD prevé que cuando el interesado ya disponga de la información el responsable estará exceptuado de otorgarle la información. La expresión "en la medida en que" del artículo 13.4 del RGPD se refiere a que, incluso aunque el interesado haya recibido parte de la información, el responsable del tratamiento deberá completar dicha información para garantizar que el interesado dispone actualmente de toda la información requerida por la normativa. En el caso de que se afirme que ya dispone de toda la información, el responsable deberá poder demostrarlo. En el caso de que no esté totalmente seguro de que el interesado tenga la información previamente, deberá proporcionarle toda la información.

También estará exceptuado el responsable de su obligación de informar cuando la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de investigación científica, o en la medida en que pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. La imposibilidad o el esfuerzo desproporcionado solo será aplicable cuando los datos personales se obtuvieron de una fuente distinta del interesado, puesto que el artículo 14 se refiere a los datos personales que no se hayan obtenido del interesado[477].

La imposibilidad se da muy pocas veces en la práctica. Esta excepción puede ocurrir cuando el responsable del tratamiento no tiene los datos de contacto de las personas y no tiene medios razonables para obtenerlos, pero no siempre cabe esta excepción[478]. Si el responsable del tratamiento determina que es imposible proporcionar la información a las personas, deberá publicar la información de privacidad (por ejemplo, en su página web) y realizar una evaluación de impacto de protección de datos.

Nótese que al efecto el responsable del tratamiento deberá poder demostrar cuál es el factor que le impide cumplir con su obligación. Si pasado un tiempo dicho impedimento desaparece, el responsable recupera su obligación de informar al interesado inmediatamente.

---

[476] ICO., "Are there any exceptions or exemptions?", *ico*, disponible en: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/ *[Última consulta: 25 de junio de 2021]*

[477] GT29. Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, *cit.*, p.34

[478] La Autoridad de Protección de Datos de Polonia (UODO) sancionó a una empresa privada que trabajaba con datos de fuentes disponibles públicamente por no informar a más de 6 millones de personas. El responsable del tratamiento informó a las personas cuyas direcciones de correo electrónico tenía a su disposición. En el caso de las personas restantes, el responsable no cumplió debido a los altos costos operativos y en su lugar presentó la información en página web. Sin embargo, en opinión del presidente, dicha acción fue insuficiente. En consecuencia, el responsable del tratamiento debe tener mucho cuidado al confiar que se cumple la excepción de imposibilidad, ni siquiera el alto costo operativo de proporcionar la información a los interesados es una razón que justifique la imposibilidad automáticamente. Véase al respecto: UODO., "The first fine imposed by the President of the Personal Data Office", *uodo*, 3 de junio de 2019, disponible en: https://uodo.gov.pl/en/553/1009 *[Última consulta: 26 de junio de 2021]*

En cuanto al esfuerzo desproporcionado, el RGPD exige que el responsable del tratamiento debe analizar si existe un equilibrio entre el esfuerzo que implica proporcionar a las personas la información de protección de datos y el efecto que tendrá sobre ellos el uso de sus datos personales. Cuanto más significativo sea el efecto, menos probable será que pueda confiar en esta excepción. El responsable no puede basarse en esta excepción para eludir sus obligaciones. Debe poder justificar por qué ponerse en contacto con las personas es realmente desproporcionado.

En base al artículo 14.5.c) del RGPD, el responsable del tratamiento no tendrá que informar al interesado cuando la obtención o la comunicación de los datos personales esté expresamente establecida por el Derecho de la Unión o de los Estados miembros. En este caso, deberá asegurarse de que la ley en cuestión realmente le impone un requisito para obtener o divulgar los datos personales de una persona.

Por último, según recoge el artículo 14.5.d) del RGPD, el responsable estará exceptuado de su deber de informar cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria. Esto es, cuando una norma del Derecho de la Unión o de un Estado miembro obliga al responsable a no informar sobre el tratamiento al interesado, como en el caso del deber de secreto profesional establecido para determinadas profesiones cuyo revelamiento podría perjudicar a terceros. Por ejemplo, dado que los médicos están sujetos a la obligación de secreto profesional, si un paciente informa a su médico sobre una afección genética que comparte con ciertos familiares, y le facilita ciertos datos personales de los mismos, el profesional médico no informará a los parientes. Si el profesional médico lo hiciese, estaría violando la obligación de secreto profesional que le debe a su paciente[479].

6. LA PROTECCIÓN DE DATOS DESDE EL DISEÑO Y POR DEFECTO COMO OBLIGACIÓN LEGAL PREVENTIVA:

El RGPD introdujo en su artículo 25 la figura de "la protección de datos desde el diseño y por defecto" (en adelante, PddDpD), que tiene como objetivo aplicar las medidas técnicas y organizativas necesarias y adecuadas en cada caso para garantizar la protección de los datos antes de que se realice su tratamiento sin que el interesado tenga realizar ninguna acción.

El objetivo de esta disposición es velar por una protección adecuada y efectiva de los datos desde el diseño y por defecto, lo que significa que los responsables del tratamiento deben poder acreditar que han incorporado las medidas oportunas y las garantías necesarias en el tratamiento para que los principios de protección de datos y los

[479] GT29. Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, *cit.*, p. 38

derechos y libertades de los interesados sean efectivos[480]. Por ello, ha sido introducido para la implementación efectiva de la responsabilidad proactiva[481].

De esta manera, se aleja de una lectura estricta del sistema individualista, puesto que se trata de una obligación que la normativa impone al responsable del tratamiento. Mediante esta figura, el legislador apuesta por proteger el entorno que rodea a la solicitud del consentimiento del interesado, en vez de limitarse a robustecer sus requisitos.

Este concepto se compone de dos elementos: la "protección de datos desde el diseño" en adelante PddD, y la "protección de datos por defecto", en adelante PdpD. El primero se refiere a la incorporación de las medidas necesarias para que el derecho a la protección de datos sea respetado a lo largo de todo el ciclo de vida del objeto. Por su parte, el segundo elemento, la protección de datos por defecto, se refiere a las decisiones relativas a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Veamos a continuación a qué corresponden ambas figuras.

6.1. La protección de datos desde el diseño:

Se ha dicho que la PddD es una cuestión de estrategia que el responsable del tratamiento debe desplegar para asegurarse de que el derecho fundamental a la protección de datos mediante la adopción e implementación de medidas técnicas y organizativas que consideren a la persona, titular de los datos personales desde el principio[482] y hasta el final del tratamiento de los datos personales. En este sentido, los expertos han señalado que las tecnologías deben ser construidas teniendo en cuenta la necesidad de la protección de los derechos del usuario[483]. Operar desde el momento del diseño inicial y del desarrollo de una tecnología teniendo en consideración el derecho a la protección de datos como un elemento más para su buen funcionamiento, responde a una visión de

[480] Los principios de protección de datos se recogen en el artículo 5 del RGOD mientras que los derechos y libertades de los interesados son los derechos y libertades fundamentales de las personas físicas, y en particular su derecho a la protección de sus datos personales. Véase al respecto: CEPD. Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto, 20 de octubre de 2020, pp. 5 y 7

[481] La responsabilidad proactiva se refiere a la obligación del responsable del tratamiento de respetar los principios del tratamiento de datos recogidos en el artículo 5.1. del RGP, y a la capacidad de demostrar dicho cumplimiento. Esto es, la obligación que tiene el responsable del tratamiento de datos de aplicar medidas técnicas y organizativas adecuadas con el objetivo de garantizar y poder demostrar que el tratamiento de datos personales es conforme con el Reglamento.

[482] RECIO GAYO, M., "Protección de datos desde el diseño: principio y obligación en el RGPD", *elderecho*, 20 de febrero de 2017, disponible en: https://elderecho.com/proteccion-de-datos-desde-el-diseno-principio-y-obligacion-en-el-rgpd *[Última consulta: 3 de julio de 2021]*

[483] GIL GONZÁLEZ, E., *Big data, privacidad y protección de datos*, *cit.*, p. 135

prevención y de reducción de riesgos que puede limitar en gran medida la vulneración de derechos en este contexto[484].

En esta línea, el apartado 1 del artículo 25 del RGPD recoge la definición de la protección de datos desde el diseño (PddD), que está orientado a establecer estrategias que incorporen medidas para respetar el derecho a la protección de datos a lo largo de todo el ciclo de vida del objeto, ya sea este un sistema, un servicio un producto hardware o software o un proceso. Se entiende por ciclo de vida del objeto todas las etapas por las que atraviesa este, desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada. Además, deben contemplarse los procesos y prácticas involucradas en el tratamiento de datos asociados, logrando así una verdadera gobernanza de la gestión de los datos personales por parte de los responsables[485].

Tal como exige el Reglamento, los responsables del tratamiento deben aplicar "medidas técnicas y organizativas apropiadas" e integrar "las garantías necesarias" para aplicar los principios que se recogen en el RGPD. La obligación de adoptar políticas internas y aplicar medidas que cumplan en particular los principios de PddD recae sobre el responsable del tratamiento. La normativa no recoge una lista con las medidas y garantías apropiadas, sino que otorga libertad a los responsables para que estos decidan cuáles son las adecuadas para el caso concreto. Por otra parte, es importante señalar que el responsable no podrá delegar completamente sus obligaciones de aplicación de este principio, ya que siempre quedará bajo su poder de decisión el establecimiento de las medidas organizativas que le compete tomar para interaccionar con el servicio subcontratado[486].

Por otra parte, en el Considerando 78 del RGPD se establece que ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función. Por ejemplo, una empresa que pretenda crear un nuevo IdC para el tratamiento de datos de salud, deberá analizar cómo va a afectar el dispositivo a los derechos y libertades de los futuros usuarios, y adoptar e implementar las medidas técnicas y organizadas apropiadas desde el diseño del producto. En este sentido, ingenieros e informáticos, entre otros perfiles técnicos, reclaman formación específica

[484] DUASO CALÉS, R., "Los principios de protección de datos desde el diseño y protección de datos por defecto", en PIÑAR MAÑAS, J.L., *Reglamento General de Protección de Datos. Hacia un nuevo modelo de Privacidad*, Reus, Madrid, 2016, p. 316

[485] AEPD. Guía de privacidad desde el diseño, 5 de octubre de 2019, pp. 6-7

[486] AEPD., "Medidas de protección de datos desde el diseño y por defecto", *aepd*, 27 de febrero de 2020, disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/proteccion-de-datos-diseno-por-defecto *[Última consulta: 1 de julio de 2021]*

en ética y protección de los datos personales que no se encuentra en los planes docentes[487].

En cuanto a las medidas técnicas y organizativas apropiadas y a las garantías necesarias, el artículo 25.1 del RGPD no ofrece un listado, quedando una vez más en manos del responsable del tratamiento su adopción. No obstante, el Reglamento se refiere expresamente a la seudonimización y a la minimización de datos como ejemplos de dicha práctica. La seudonimización está recogida en el artículo 32.1.a) del RGPD como una medida técnica apropiada en el apartado relativo a la seguridad de los datos personales. Como se ha dicho anteriormente, esta técnica se utiliza para que un dato personal no pueda ser atribuido a un interesado sin agregar información adicional. Por su parte, la minimización de datos tiene como objetivo que los datos a tratar sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. En este sentido, la Comisión Europea, en su comunicación relativa a las orientaciones sobre las aplicaciones móviles de apoyo a la lucha contra la pandemia de Covid-19 en lo referente a la protección de datos 2020/C 124 I/01, de 17 de abril de 2020, identifica, entre otros, a la seudonimización[488] y a la minimización[489] como elementos para un uso fiable y responsable de las aplicaciones[490].

Para que sean apropiadas, las medidas y las garantías necesarias deben ser idóneas para conseguir el fin previsto, deben aplicar los principios de protección de datos de forma efectiva. Por ello, el requisito de que sean apropiadas está estrechamente ligado al requisito de la efectividad. Una medida técnica u organizativa o una garantía puede ser cualquier cosa desde la aplicación de soluciones técnicas avanzadas hasta la formación básica del personal. Las empresas deberán adoptar políticas internas, utilizar técnicas innovadoras y realizar evaluaciones de impacto[491] para cumplir con esta obligación[492].

---

[487] DE LECUONA, I. "Aspectos éticos, legales y sociales del uso de la inteligencia artificial y el Big Data en salud en un contexto de pandemia", *Revista Internacional de Pensamiento Político*, Núm. 15, 2020, p. 151

[488] En el punto 3.8 de la comunicación, la Comisión expone que los datos de proximidad solo deben generarse y almacenarse en el dispositivo terminal de la persona en un formato cifrado y seudonimizado. Asimismo, cuando la legislación nacional establezca que los datos personales recogidos también pueden tratarse con fines de investigación científica, se deberá utilizar, en principio, la seudonimización.

[489] En base al principio de minimización, en el artículo 3.4 de la comunicación, la Comisión aconseja el uso de Bluetooth de baja energía en vez de la geolocalización a efectos de medir la proximidad y los contactos estrechos para interrumpir la cadena de infección. Según afirma, los datos de localización no son necesarios para los fines de las funcionalidades de rastreo de contactos, ya que su objetivo no es ni seguir los movimientos de las personas ni controlar el cumplimiento de las prescripciones. Por ello, el tratamiento de los datos de localización en el marco del rastreo de contactos es difícilmente justificable a la luz del principio de minimización de datos.

[490] En este aspecto, se ha expuesto que la aplicación informática "RADAR COVID" es un claro ejemplo de la opacidad y falta de transparencia. La app recomendada por el gobierno español para la identificación de posibles positivos y el rastreo de sus contactos no ha sido objeto de un debate social informado acerca de su diseño, validación e implementación. Véase al respecto: DE LECUONA, I. "Aspectos éticos, legales y sociales del uso de la inteligencia artificial y el Big Data en salud en un contexto de pandemia", *cit.*, p. 148

[491] Artículo 35 del RGPD

[492] ROMANOU, A., "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise", *Computer law & security review*, Vol. 34, Núm. 1, 2018, p. 102

En pocas palabras, el PddD tiene como objetivo que el derecho fundamental a la protección de datos personales sea uno de los aspectos esenciales a incluir en cualquier plan de negocio o diseño de una aplicación, servicio o producto, ya que ello facilitará desarrollar el programa de cumplimiento que permita, al mismo tiempo, generar o impulsar la confianza de los interesados. Por tanto, la PddD es una cuestión de estrategia que el responsable del tratamiento debe tener en consideración para asegurar el derecho fundamental a la protección de datos mediante la adopción e implementación de medidas técnicas y organizativas que consideren a la persona, titular de los datos personales desde el principio[493] y hasta el final del tratamiento de los datos personales.

El PddD se compone de siete características: es proactivo y preventivo; el derecho a la protección de datos es la configuración predeterminada; el derecho a la protección de datos está incorporado al diseño; la funcionalidad es total; el derecho a la protección de datos está asegurado durante todo el ciclo de vida; es visible y transparente, y el enfoque está centrado en el titular de los datos.

Respecto a la primera característica, el enfoque de PddD no espera a que se materialicen los riesgos, ni ofrece remedios para resolver infracciones una vez que han ocurrido, tiene como objetivo evitar que ocurran. La protección de datos desde el diseño viene antes del hecho, no después[494]. Cualquier sistema, aplicación, servicio o producto que vaya a utilizar datos personales debe ser concebida y diseñada desde cero identificando los posibles riesgos a los derechos y libertades de los interesados y minimizarlos para que no lleguen a concretarse en daños[495]. Esto es, a través de la PddD, el RGPD instaura un modelo de cumplimiento preventivo y proactivo en lugar de defensivo y sancionador[496]. Es una manera de prevenir e impedir el daño, en vez de repararlo una vez se haya producido.

A su vez, la configuración predeterminada será aquella que respete lo máximo posible el derecho a la protección de datos del titular de los datos, no se requiere ninguna acción por parte de este último[497]. Aunque la persona no realice ninguna acción su derecho a la protección de datos se mantiene intacto, dado que se encuentra predeterminado. En consecuencia, los datos personales deberán estar automáticamente protegidos en cualquier sistema tecnológico[498]. Este elemento puede ser comprendido como el principio de la PdpD.

---

[493] RECIO GAYO, M., "Protección de datos desde el diseño: principio y obligación en el RGPD", *elderecho*, 20 de febrero de 2017, disponible en: https://elderecho.com/proteccion-de-datos-desde-el-diseno-principio-y-obligacion-en-el-rgpd *[Última consulta: 3 de julio de 2021]*

[494] CAVOUKIAN, A., "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian", D. *Identity in the Information Society*, Vol. 3, Núm. 2, 2010, p. 249

[495] AEPD. Guía de privacidad desde el diseño, *cit.*, p.7

[496] GARCÍA MEXÍA, P. y PERETE RAMÍREZ, C., "Internet y el Reglamento General de Protección de Datos", en LÓPEZ CALVO, J. (coord), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Bosch, Madrid, 2018, p. 180

[497] CAVOUKIAN, A., "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian", *cit.*, pp. 250

[498] AEPD. Guía de privacidad desde el diseño, *cit.*, p.8

El tercer requisito se refiere a que el derecho a la protección de datos debe estar incorporado al diseño, no debiendo ser visto como un agregado, será parte inseparable de la solución desarrollada, planteada desde su creación[499]. Debe formar parte integral e indisoluble de los sistemas, aplicaciones, productos y servicios, así como de las prácticas de negocio y procesos de la organización. No es una capa adicional o módulo que se añade a algo preexistente, sino que debe estar integrada en el conjunto de requisitos no funcionales desde el mismo momento en el que se concibe y diseña[500].

La funcionalidad debe ser total. Tradicionalmente se ha entendido que se gana el derecho a la protección de datos a costa de perder otras funcionalidades, presentando dicotomías como derecho a la protección de datos vs usabilidad, derecho a la protección de datos vs funcionalidad, derecho a la protección de datos vs beneficio empresarial, incluso derecho a la protección de datos vs seguridad. Esta aproximación es artificial y el objetivo ha de ser buscar el balance óptimo en una búsqueda tipo "*win-win*" o "gana-gana", con una mentalidad abierta a nuevas soluciones para conseguir sistemas plenamente funcionales, eficaces y eficientes también a nivel del derecho a la protección de datos[501]. En esta dinámica ganan ambas partes, tanto organizaciones como los interesados[502]. Un producto, servicio o aplicación puede estar plenamente operativo con todas las funcionalidades activas, sin dejar a un lado los derechos de los usuarios.

Asimismo, el derecho a la protección de datos debe estar asegurando durante todo el ciclo de vida del sistema, aplicación, servicio o producto**.** Las estrategias que incorporen el derecho a la protección de datos deberán estar establecidas a lo largo de todo el ciclo de vida del mismo. Para ello, se deben analizar detenidamente las distintas operaciones e implementar, en cada una de ellas, las medidas más adecuadas para proteger los datos[503].

En cuanto a la visibilidad y transparencia, el responsable del tratamiento debe actuar en base a los objetivos marcados, e igualmente ha de ser capaz de demostrar que ha incluido satisfactoriamente todas las medidas necesarias. Su ejercicio ha de ser transparente. Mediante esta característica se pretende lograr una confianza en el sistema. Por último, el enfoque está centrado en el titular de los datos, aunque cada organización tenga sus objetivos, la principal finalidad debe ser garantizar los derechos y libertades de los interesados[504]. Los mejores resultados se logran cuando el diseño se realiza en torno a los intereses y necesidades de los interesados.

---

[499] OSTEC., "¿Qué significa "privacy by design" y cuál es su relación con la ley de protección de datos?", *ostec*, 29 de julio de 2019, disponible en: https://ostec.blog/es/generico/privacy-by-design/ *[Última consulta: 3 de julio de 2021]*

[500] AEPD. Guía de privacidad desde el diseño, *cit.*, p.8

[501] Ibid., pp.8-9

[502] GIL GONZÁLEZ, E., *Big data, privacidad y protección de datos*, *cit.*, p. 136

[503] AEPD. Guía de privacidad desde el diseño, *cit.*, p.9

[504] CAVOUKIAN, A., "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian", *cit.*, pp. 250

El artículo 25, apartado 1, enumera los elementos que el responsable del tratamiento debe tener en cuenta a la hora de determinar las medidas de una operación específica de tratamiento: el estado de la técnica; el coste de la aplicación; la naturaleza, ámbito, contexto y fines del tratamiento; y los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas.

El estado de la técnica se refiere a la obligación de los responsables del tratamiento de tener en cuenta el progreso actual de la tecnología disponible en el mercado a la hora de determinar las medidas técnicas y organizativas adecuadas. Lo que se exige mediante este elemento es que los responsables del tratamiento conozcan y se mantengan al día de los avances tecnológicos, de cómo la tecnología puede presentar riesgos u oportunidades para la protección de datos, y de cómo aplicar las medidas y garantías que aseguran la aplicación efectiva de los principios y derechos de los interesados teniendo en cuenta la evolución del panorama tecnológico. Asimismo, este criterio también se aplica a las medidas de carácter organizativo como las relativas a formaciones de reciclaje tecnológica. La falta de medidas organizativas adecuadas puede reducir o incluso restar toda efectividad a la tecnología elegida[505].

Respecto al coste de la aplicación de las medidas, este hace referencia a los recursos en general, incluidos el tiempo y los recursos humanos que posee el responsable del tratamiento. Las medidas elegidas por el responsable del tratamiento garantizarán que la actividad de tratamiento de datos personales no incumpla los principios. Para ello, los responsables deben ser capaces de gestionar los costes totales para poder aplicar todos los principios de forma efectiva[506].

En cuanto al tercer elemento, los responsables deben tomar en consideración la naturaleza, ámbito, contexto y fines del tratamiento de datos personales para determinar las medidas que han de ser adoptadas. Es necesario que el responsable analice adecuadamente las características del tratamiento de datos personales que se realizará para entender el impacto que tendrá dicho tratamiento en el derecho a la protección de datos del interesado. En este sentido, no es lo mismo tratar un dato personal "normal" que uno sensible, como por ejemplo un dato sanitario.

Por último, el responsable del tratamiento tiene que determinar los riesgos que entraña una violación de los principios para los derechos de los interesados, así como su probabilidad y gravedad a fin de aplicar medidas que mitiguen de forma efectiva los riesgos detectados. En este sentido, se ha identificado a la evaluación de impacto como elemento clave para la correcta implantación de la PddD. Se trata de la realización de un análisis de los riesgos que un nuevo servicio, producto o aplicación puede suponer para el derecho a la protección de datos de los interesados, de manera que tras la realización de ese análisis se pueda realizar un plan de acción para eliminar o, al menos, reducir a niveles aceptables los riesgos identificados. Persigue identificar e implementar medidas

[505] CEPD. Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto, *cit.*, pp.8-9
[506] Ibíd., p. 9

orientadas a eliminar o mitigar los riesgos con carácter previo a la puesta en marcha de aquellos tratamientos que sea probable que conlleven un alto riesgo para los derechos y libertades de los interesados[507]. La EIPD sigue el enfoque proactivo del PddD, y por ello se considera un elemento clave para su correcta implantación.

6.2. La protección de datos por defecto:

En el ámbito informático, el término "por defecto" se refiere al valor preexistente o preseleccionado de un parámetro configurable que se asigna a una aplicación informática, a un programa informático o a un dispositivo periférico. Estos parámetros se denominan "preajustes" o "ajustes de fábrica", especialmente en dispositivos electrónicos. En base a la protección de datos por defecto (PdpD), cuando una aplicación informática, un servicio o un dispositivo salen al mercado, se deben aplicar las configuraciones más estrictas de manera predeterminada[508], sin que el interesado tenga que realizar ninguna acción[509].

Según dicho principio los responsables solo podrán tratar los datos personales que por defecto sean estrictamente necesarios para cada uno de los fines de tratamiento[510]. Esto es aplicable, como se ha expuesto, a la cantidad de los datos recogidos, los tratamientos que realizan, el tiempo de conservación y el acceso a los mismos. Así, el responsable del tratamiento no puede recoger más datos personales de los que necesita, realizar un tratamiento más amplio de lo necesario para lograr los fines establecidos, ni conservar los datos personales más tiempo de lo necesario. Por tanto, las aplicaciones informáticas, solo podrán acceder a los datos que realmente necesitan para poner a disposición del usuario una función[511].

La configuración establecida debe ser siempre la más protectora de los intereses del interesado, de forma que ningún titular de los datos pueda por defecto verse expuesto a diferentes riesgos que ignora o que no sabe valorar en su justa medida[512]. Pero la aplicación puede permitir que este pueda cambiar la configuración por defecto para

---

[507] CABEZAS VÁZQUEZ, R., "Proteger la privacidad desde el diseño del producto", *Cincodías.elpaís*, 31 de julio de 2019, disponible en: https://cincodias.elpais.com/cincodias/2019/07/30/companias/1564510266_593013.html *[Última consulta: 5 de julio de 2021]*

[508] Un estudio puso de manifiesto que la aplicación de mensajería WhatsApp Messenger no cumple este principio. Cuando se instala esta aplicación, por defecto, cualquier persona que tenga el contacto de otra podrá ver su estado, foto de perfil y la última vez que se conectó. Es el interesado el que tiene que cambiar manualmente la configuración. Véase al respecto: MOJICA LOPEZ, M.; RODRIGO OLIVA, J.L.; GAYOSO MARTÍNEZ, V.; HERNANDEZ ENCINAS, L. y MARTÍN MUÑOZ, A., "Análisis de la privacidad de WhatsApp Messenger", *Revista de sistemas, cibernética e informática*, Vol. 14, Núm. 2, 2017, p. 74

[509] ICS., "What is privacy by design & default?", *ics*, disponible en: https://www.ics.ie/news/what-is-privacy-by-design-a-default *[Última consulta: 8 de julio de 2021]*

[510] EDPS., "Privacy by default", *edps*, disponible en: https://edps.europa.eu/data-protection/our-work/subjects/privacy-default_en *[Última consulta: 9 de julio de 2021]*

[511] GT29. Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, *cit.*, p. 23

[512] DUASO CALÉS, R., "Los principios de protección de datos desde el diseño y protección de datos por defecto", *cit.*, p. 310

permitir otras utilidades que requieran un nivel de protección menor[513]. Así, el interesado podrá autoriza que se procesen más datos personales, ampliar la extensión del tratamiento, que los datos se conserven durante un tiempo mayor y que otras terceras personas puedan acceder a sus datos personales.

En el segundo párrafo del artículo 25 del RGPD no se incorporan ejemplos de cuáles son las medidas técnicas y organizativas apropiadas. Al igual de lo que ocurre en la PddD, corresponde al responsable del tratamiento implementar medidas técnicas y organizativas adecuadas para asegurarse de que solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento[514].

Respecto a la extensión del tratamiento, el responsable se limitará a lo estrictamente necesario para cumplir con el propósito declarado ante el interesado[515]. En consecuencia, el término "cantidad" implica tanto factores cualitativos como cuantitativos de los datos. El responsable del tratamiento deberá considerar el volumen de datos personales tratados, el nivel de detalle, las diferentes categorías, la sensibilidad (categorías especiales de datos) y los tipos de datos personales requeridos y necesarios para llevar a cabo una operación de tratamiento, incluyendo tanto los datos recogidos como los generados o inferidos a partir de estos[516].

Respecto a la extensión del tratamiento, se refiere a que los tratamientos realizados por el responsable se limitarán a lo estrictamente necesario para cumplir con el propósito declarado por este[517]. En consecuencia, en todas las fases que componen el tratamiento deberán realizarse únicamente las operaciones necesarias, y sobre los datos necesarios para el cumplimiento de la finalidad de dichas fases. En particular, el responsable y, en los casos oportunos, el usuario, han de poder configurar la extensión del tratamiento en cada fase, en particular en función de los casos de uso[518].

Además, el responsable del tratamiento deberá limitar el período de conservación de los datos personales a lo estrictamente necesario para el fin previsto. Cuando los datos personales dejen de ser necesarios para la finalidad del tratamiento, serán suprimidos o anonimizados. Esta acción se realizará por defecto, es decir, el responsable del tratamiento debe contar con procedimientos automáticos para suprimir o anonimizar los datos. Esta obligación está directamente relacionada con el principio de limitación del

---

[513] NOAIN-SÁNCHEZ, A., "Privacy by default and active informed consent by layers: Essential measures to protect ICT users' privacy", *Journal of Information, Communication and Ethics in Society*, Vol.14, Núm.2, 2016, p. 130

[514] HANSEN, M., *Data protection by design and by default à la European General Data Protection Regulation*, Springer, Cham, 2016, p. 33

[515] CEPD. Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto, *cit.*, p. 13

[516] AEPD. Guía de privacidad desde el diseño, cit., p. 21

[517] ECONOMIST & JURIST., "5 preguntas sobre la nueva guía de protección de datos por defecto", *economistjurist*, 11 de noviembre de 2020, disponible en: https://www.economistjurist.es/noticias-juridicas/5-preguntas-sobre-la-nueva-guia-de-proteccion-de-datos-por-defecto/ *[Última consulta: 10 de julio de 2021]*

[518] AEPD. Guía de privacidad desde el diseño, cit., p. 21

plazo de conservación establecido en el artículo 5.1.e) del RGPD[519]. Nótese que, es la finalidad del tratamiento en cuestión la que hace que la duración del período de conservación varíe[520].

Por último, el responsable del tratamiento decidirá quién tiene acceso a los datos personales y qué tipo de acceso se concede a estos terceros autorizados. Estas cesiones implican que deben observarse controles de acceso para todo el flujo de datos durante el tratamiento[521]. Cumpliendo con la obligación de informar y de recabar el consentimiento del interesado, se consultará al interesado antes de hacer accesibles los datos a terceras personas. El tratamiento ha de ser configurable por el responsable, y en su caso por el usuario, para ajustar el grado de accesibilidad a los distintos casos de uso.

6.3. El mecanismo de la certificación:

El legislador introdujo en el tercer y último apartado del artículo 25 del RGPD el mecanismo de la certificación para poder acreditar el cumplimiento de la protección de datos desde el diseño y por defecto con arreglo artículo 42 del mismo cuerpo legal. En este último apartado se recoge que los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el RGPD en las operaciones de tratamiento de los responsables y los encargados, y que se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

La Organización Internacional de Normalización, más conocida como ISO ("*International Organization of Standardization*"),[522] define la certificación como una declaración que demuestra que un producto, proceso o sistema cumple unos requisitos especificados[523].

El RGPD no define que son los certificados, sellos o marcas, y utiliza los citados términos conjuntamente. Sello o marca se refiere habitualmente a un logotipo o símbolo que indica que el objeto de certificación ha sido valorado de forma independiente en un

[519] El principio de limitación del plazo de conservación está íntimamente relacionado con el principio de minimización. Al igual que solo pueden tratarse los datos adecuados, pertinentes y necesarios para una finalidad, la conservación de esos datos debe limitarse en el tiempo al logro de los fines que el tratamiento persigue. Una vez que esas finalidades se han alcanzado, los datos deben ser borrados o, al menos, desprovistos de todo elemento que permita identificar a los interesados. Véase al respecto: AEPD., "Principios", *cit.*

[520] CEPD. Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto, *cit.*, p. 14

[521] Ibíd.

[522] Se trata de una una organización para la creación de estándares internacionales compuesta por diversas organizaciones nacionales de normalización. Es una red mundial que identifica qué normas internacionales son requeridas por el comercio, los gobiernos y la sociedad. Véase al respecto: ISO., "Organismos Nacionales de Normalización en Países en Desarrollo", *iso*, p. 1, disponible en: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/fast_forward-es.pdf

[523] ISO/IEC 17000:2004. Evaluación de la conformidad. Vocabulario y principios generales, p. 4

procedimiento de certificación y es conforme a los requisitos especificados, enunciados en documentos normativos como reglamentos, normas o especificaciones técnicas. Por ello, un certificado, sello o marca puede emitirse únicamente tras la evaluación independiente de las pruebas por parte de un organismo acreditado de certificación o autoridad de control competente que indique que los criterios de certificación se han cumplido[524].

Se ha dicho que el Reglamento introdujo la certificación como medio para demostrar el cumplimiento y para generar confianza en la sociedad[525]. En este sentido, el artículo 24.3 del RGPD establece que los mecanismos de certificación pueden ser utilizados para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento. Esta demostración del cumplimiento requiere documentación justificativa, especialmente informes por escrito que describan cómo se cumplen los criterios y si inicialmente no se cumplían, describan las correcciones y acciones correctivas y su idoneidad, proporcionando así motivos para otorgar y mantener la certificación. Esto incluye el resumen de la decisión concreta por la que se otorga, renueva o retira un certificado[526].

Por su parte, el Considerando 100 del Reglamento afirma que a fin de aumentar la transparencia y el cumplimiento del RGPD, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes[527]. Por todo ello, puede afirmarse que se trata de un sistema inspirado en los mecanismos de certificación de calidad industrial[528].

La certificación será expedida por los organismos de certificación, por la autoridad de control competente o por el CEPD[529]. En base al artículo 43.1 del RGPD, los organismos de certificación que tengan un nivel adecuado de pericia en materia de protección de datos podrán expedir y renovar las certificaciones una vez informada la autoridad de control. No obstante, para poder desempeñar dichas funciones, deberán ser acreditados por la autoridad de control competente o por el organismo nacional de

[524] CEPD. Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículo 42 y 43 del Reglamento, 4 de junio de 2019, p. 9

[525] FERNÁNDEZ SÁNCHEZ, C. y RECIO GAYO, M., "Certificación en protección de datos personales", en PIÑAR MAÑAS, J.L., *Reglamento General de Protección de Datos. Hacia un nuevo modelo de Privacidad*, Reus, Madrid, 2016, pp.413-414

[526] CEPD. Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículo 42 y 43 del Reglamento, *cit.*, p. 8

[527] En el ámbito específico de las aplicaciones móviles sanitarias, como bien se ha indicado en el primer capítulo del presente trabajo, la Agencia de Calidad Sanitaria de Andalucía otorga el Distintivo "*AppSaludable".* Con dicho distintivo se reconoce a aquellas aplicaciones de salud que ponen en marcha las medidas necesarias para cumplir una serie de recomendaciones de calidad y seguridad y que, por tanto, pueden ser utilizadas por la ciudadanía de forma fiable, minimizando riesgos.

[528] FERNÁNDEZ VILLAZÓN, L. A. "El nuevo reglamento europeo de protección de datos". *Foro. Revista de Ciencias Jurídicas y Sociales, Nueva Época, Vol. 19, Núm. 1, 2016,* p. 403; TIKKINEN-PIRI, C.; ROHUNEN, A. y MARKKULA, J., "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Computer Law & Security Review*, Vol. 34, Núm. 1, 2018, p. 138

[529] Artículo 42.5 del RGPD

acreditación[530]. Las autoridades de control tratarán todas las solicitudes de aprobación de criterios de certificación de forma justa y no discriminatoria, de acuerdo con un procedimiento de acceso público que especifique las condiciones generales que deben cumplirse y la descripción del proceso de aprobación[531]. La acreditación se obtendrá por un periodo máximo de 5 años, aunque podrá ser renovada siempre y cuando se sigan cumpliendo los requisitos. En el caso de que no cumplan los requisitos, la autoridad de control competente o el organismo nacional de acreditación podrá revocar la acreditación[532]. Para lograr la certificación, los responsables y encargados han de facilitar toda la información y acceso a las actividades de tratamiento al organismo de certificación.

Tal y como se indica en el artículo 43.5 del RGPD, antes de expedir la certificación o proceder a su retirada, los organismos de certificación deben comunicar a la autoridad de control competente en qué se han basado a la hora de tomar dicha decisión[533]. En esta revisión, se tienen en cuenta las normas y procedimientos en virtud de los cuales los organismos emitirán los certificados, sellos o marcas[534].

Las autoridades de control competentes también podrán actuar como organismo de certificación, debiendo de emitir (artículo 58.2.f del RGPD), revisar (artículo 57.1.o del RGPD y retirar (artículo 58.2.h del RGPD) las certificaciones. Asimismo, en base al artículo 58.3.f) del RGPD, corresponde a las autoridades de control competente aprobar los criterios de certificación. Estos criterios de certificación deben formularse de manera que sean claros y comprensibles y que permitan su aplicación práctica.

En cuanto al CEPD, le corresponde acreditar a los organismos de certificación, revisarlos y llevar un registro público de los organismos acreditados[535]. Igualmente, será el CEPD quien deba aprobar los criterios de certificación. El RGPD incorpora un sello Europeo de Protección de Datos es un certificado de privacidad, protección de datos y seguridad, transparente e independiente, para productos y servicios tecnológicos

[530] En aplicación del Reglamento (CE) nº 765/2008 que regula el funcionamiento de la acreditación en Europa, la Entidad Nacional de Acreditación (ENAC) es la entidad designada por el Gobierno español para operar en España como el único Organismo Nacional de Acreditación. La solicitud de acreditación es analizada por los técnicos de ENAC. Si el resultado de la evaluación es positivo, la organización de certificación será acreditada. Dicha acreditación será reevaluada regularmente con la finalidad de comprobar que la organización de certificación mantiene la competencia técnica necesaria. Véase al respecto: FERNÁNDEZ SÁNCHEZ, C. y RECIO GAYO, M., "Certificación en protección de datos personales", *cit.*, pp.422-423

[531] CEPD. Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículo 42 y 43 del Reglamento, *cit.*, p. 13

[532] Artículo 43.7 del RGPD

[533] En base al artículo 39 de la LOPDGDD, ENAC deberá comunicar a la AEPD y a las autoridades de protección de datos de las comunidades autónomas las concesiones, denegaciones o revocaciones, así como su motivación.

[534] CEPD. Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículo 42 y 43 del Reglamento, *cit.*, p. 12

[535] Artículo 70.1.o) del RGPD

en el entorno europeo[536]. Esta certificación se otorgará en dos fases: en primer lugar, una evaluación del producto o servicio a certificar, evaluación realizada por expertos jurídicos e informáticos. Realizada esta evaluación, estos expertos evacuan un informe que debe ser revisado por una entidad de certificación, para posteriormente, y siempre y cuando se cumpla con la normativa europea, otorgar el Sello Europeo de Privacidad[537]. Según el Reglamento, corresponde al CEPD archivar en un registro todos los mecanismos de certificación y sellos de protección de datos y los ponerlos a disposición pública por cualquier medio apropiado.

Según el artículo 42.3 del RGPD, la certificación es voluntaria. La certificación no limita la responsabilidad del responsable del tratamiento en cuanto al cumplimiento del RGPD, sino que es utilizada para demostrar su cumplimiento. Se trata por tanto de un mecanismo que sirve para demostrar el cumplimiento de la normativa y para general confianza en el usuario, pero no exime al responsable del tratamiento de seguir cumpliendo el RGPD tras su adquisición.

6.4. La protección de datos desde el diseño y por defecto como factor innovador del consentimiento del interesado:

Como base de esta aproximación crítica se ha dicho que aunque el RGPD aboga por la utilización de un lenguaje sencillo, políticas fáciles de comprender y casillas o ventanillas fáciles de identificar en las que los usuarios pueden indicar su consentimiento, los pocos usuarios que leen las políticas de privacidad no llegan a comprenderlas realmente. Los textos escritos en este lenguaje sencillo no permiten tener información suficiente para elaborar un consentimiento informado. Se trata además, según esta perspectiva, de una misión imposible ya que el detalle que sería necesario para que la política de privacidad diera información suficiente sería abrumador [538].

En esta línea, el GT29 expresó que la complejidad de las prácticas de recogida de datos, los nuevos modelos empresariales, las relaciones con los vendedores y las nuevas aplicaciones tecnológicas llegan en muchos casos a sobrepasar la capacidad o la voluntad de la persona para tomar decisiones de control sobre el uso e intercambio de información por medio de una elección activa[539]. Es difícil pensar que, los ciudadanos puedan dedicar el tiempo necesario, ni que dispongan, al menos en la mayoría de los casos, de la formación precisa para poder comprender y valorar la información que se les facilite en el ejercicio de este derecho[540]. Igualmente, la intensificación y

[536] Véase al respecto: CAVOUKIAN, A. y CHIBBA, M., "Privacy Seals in the USA, Europe, Japan, Canada, India and Australia", en RODRIGES, R. y PAPAKONSTANTINOU, V., *Privacy and Data Protection Seals*, Asser, Berlin, 2018, p. 70

[537] EUROPEAN PRIVACY SEAL., "EuroPriSe - Sello Europeo de Privacidad", *europrivacyseal*, disponible en: https://www.euprivacyseal.com/EPS-en/Europrise-sello-europeo-de-privacidad *[Última consulta: 15 de julio de 2021]*

[538] GIL GONZÁLEZ, E., *Big data, privacidad y protección de datos*, *cit.*, 2016, p. 72

[539] GT29. Dictamen 15/2011 sobre la definición del consentimiento, *cit.*, p. 12

[540] OLIVER LALANA, A.; MUÑOZ SORO, J.F., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", en VALERO TORRIJOS, J., *La protección de datos personales en*

sofisticación de las técnicas de acopio y procesamiento de datos personales priva de opciones reales de saber y decidir que se hace con los datos personales de cada persona. La lógica subyacente, entre otros, del Big data[541] y la inteligencia artificial es tan abrumadora que incluso, como sucede con las redes neuronales, ni tan siquiera sus propios desarrolladores la dominan del todo[542].

En base a lo anterior, algunos autores defienden que, el ideal normativo de "consentimiento y control" es un mito, un mantra cuya capacidad para modelar la realidad es poca: una persona corriente no puede hoy esperar tener un control sustancial de su información ni de como la usan otros (estado, empresas y conciudadanos)[543]. La aplicación del consentimiento en la realidad tecnológica escapa de los límites de la autonomía individual[544] y el empoderamiento dentro de una sociedad moderna[545]. Así, el imperio del poder de la información ha producido una pérdida real de autocontrol[546].

Según la corriente doctrinal que estamos comentando, la mayoría de los interesados tienen un limitado conocimiento tecnológico y, por lo tanto, no están en condiciones de tomar las medidas de seguridad pertinentes por sí mismos para así proteger sus datos personales. A su vez, aun no existe una cultura arraigada de protección de datos. El hecho de que haya muchos ciudadanos para los que el bien jurídicamente protegido de la autodeterminación informativa tiene escaso valor, sobre todo cuando se confronta con otros posibles beneficios, propicia que las iniciativas empresariales más agresivas en materia de protección de datos encuentren siempre un amplio nicho entre la población que las acepta de forma acrítica[547].

Para que la legislación de protección de datos cumpla su promesa normativa de control son precisos cambios sustanciales en la industria del conocimiento. Los autores críticos

---

internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica. Aranzadi Thomson Reuters, Pamplona, 2013. p. 188

[541] La corriente doctrinal que defiende que el consentimiento individual ha fracasado como mecanismo de control critica, entre otras cuestiones, el requisito de que el consentimiento sea específico. Por ejemplo, en razón de la especial naturaleza y desarrollo del Big data, sería difícil determinar las finalidades o comunicaciones que van a producirse. Con los sistemas de inteligencia artificial y decisiones automatizadas, no es fácil consentir unas finalidades de uso de los datos que por lo general ni se conocen ni se sospechan. Véase al respecto: COTINO HUESO, L., "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata. Revista Internacional de Éticas Aplicadas*, Núm. 24, 2017, p. 145

[542] Ibid., p. 191

[543] Ibid., p. 166

[544] SCHERMER, B.W.; CUSTERS, B.; VAN DER HOF, S., "The crisis of consent: How stronger legal protection may lead to weaker consent in data protection", *cit.*, p. 171

[545] GIANNOPOULOU, A., "Algorithmic systems: the consent is in the detail?", *Internet Policy Review*, Vol. 9, Núm. 1, 2020, p. 10

[546] SANTOS DIVINO, S.B., "Reflexiones escépticas, principiológicas y económicas sobre el consentimiento necesario para la recolección y tratamiento de datos", *Derecho PUCP*, Núm. 83, 2019, p. 201

[547] OLIVER LALANA, A.; MUÑOZ SORO, J.F., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", *cit.*, p. 172; En el documental *"The social dilemma"* de la plataforma Netflix se afirma acertadamente que si no pagas por el producto, tú eres el producto. Véase al respecto: NETFLIX. "The social dilemma", *netflix*, disponible en: https://www.netflix.com/es/title/81254224

abogan por la adopción de modelos de negocio que hagan transparentes las redes telemáticas sobre las que operan, y a la postre, los intereses de quienes las controlan[548].

Es en este punto donde entra en juego la PddDpD[549]. Frente a las garantías subjetivas, que en buena medida dependen del consentimiento y la acción del individuo, se argumenta que deben reforzarse las obligaciones preventivas[550].

Hemos dicho más arriba que la protección de datos desde el diseño y por defecto son mecanismos poderosos que pueden coadyuvar a aumentar la transparencia[551]. Personalmente considero que la doctrina no le ha otorgado suficiente valor al presente concepto que realmente tiene la capacidad de cambiar la realidad actual. Es importante reforzar los requisitos del consentimiento del interesado, pero no es una medida suficiente para garantizar la autodeterminación informativa del interesado. Mediante la incorporación de los artículos 25 y 42 del RGPD, el legislador ha introducido un instrumento que ha de ser aplicado en la práctica en cumplimiento de la protección de datos desde el diseño y por defecto, lo cual se acredita mediante la herramienta de la certificación.

El interesado tiene que llegar a dar por hecho que se respetará su derecho a la protección de datos personales. Esta seguridad solo puede obtenerse a través de la concienciación de las personas y del desarrollo de ambientes que viabilicen un verdadero diálogo, donde libertades y derechos no negociables no sean moneda de cambio de los servicios ofrecidos, y es en este punto donde entra en juego el concepto de la protección de datos desde el diseño y por defecto. La tecnología ha de ser comprendida como aliada del derecho y el derecho como aliado de la tecnología[552].

En nuestra opinión a certificación es una herramienta adecuada para conseguir que el interesado confíe en el tratamiento de los datos personales que realizará el responsable del tratamiento en cuestión, puesto que se trata de un mecanismo creado por el legislador europeo para demostrar el cumplimiento de la normativa de protección de datos personales y así generar un sentimiento de seguridad en el interesado.

Por otra parte, la aplicación la protección de datos desde el diseño y por defecto beneficia a las organizaciones, puesto que, uno de los objetivos de este enfoque es la transparencia, y la transparencia es clave cuando se trata de lograr la confianza del

[548] OLIVER LALANA, A.; MUÑOZ SORO, J.F., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", *cit.*, p. 191
[549] SCHAAR, P., "Privacy by design", *Identity in the Information Society*, Vol. 3, Núm. 2, 2010, p.267
[550] COTINO HUESO, L., "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *cit.*, p. 146
[551] BOURASSA FORCIER, M.; GALLOIS, H.; MULLAN, S. y JOLY, Y., "Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?", *Journal of Law and the Biosciences*, Vol. 6, Núm. 1, 2019, pp. 332-333
[552] DE LA MATA BARRANCO, N.J. y BARINAS UBIÑAS, D., "La privacidad en el diseño y el diseño de la privacidad, también desde el derecho penal", *Eguzkilore*, Núm. 28, 2014, p. 263

posible usuario[553]. Debido al avance exponencial de la tecnología y la aparición de nuevos riesgos se requiere un nuevo enfoque. Este nuevo enfoque debe ser adaptable y debe poder evolucionar a medida que progresa la tecnología y los riesgos asociados. Esta óptica proactiva, sistemática e innovadora es la clave para que la protección de datos personales sea parte indisoluble de la cultura de las empresas y que, de esta manera, se contribuya a la creación de confianza entre los clientes, confianza que tan necesaria resulta para el despegue y correcto funcionamiento de la economía digital[554]. Así, su aplicación puede verse como una ventaja competitiva necesaria para tener éxito en el mercado[555]. En este sentido, el GT29 afirmo que a medida que ciertos certificados se vuelvan más conocidos por la rigurosidad de las pruebas de obtención, los responsables del tratamiento los preferirán por su "comodidad" de cumplimiento y la ventaja competitiva que logran con los mismos[556].

El interesado tiene que llegar a dar por hecho que se respetará su derecho a la protección de datos personales. Esta seguridad solo puede construirse a través de la concienciación de las personas y del desarrollo de ambientes que viabilicen un verdadero diálogo, donde libertades y derechos no negociables no sean moneda de cambio de los servicios ofrecidos, y es en este punto donde entra en juego el concepto de la protección de datos desde el diseño y por defecto[557]. La tecnología ha de ser comprendida como aliada del derecho y el derecho como aliado de la tecnología[558]. Por todo ello, creemos que es necesario fomentar la creación y uso en la práctica de estos certificados que declaran el cumplimiento de la normativa de protección de datos personales.

[553] DANON, S., "GDPR Top Ten #6: Privacy by Design and by Default", *deloitte*, disponible en: https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-privacy-by-design-and-by-default.html *[Última consulta: 20 de julio de 2021]*

[554] CABEZAS VÁZQUEZ, R., "Proteger la privacidad desde el diseño del producto", *cit.*

[555] CAVOUKIAN, A.; FISCHER, A.; KILLEN, S. y HOFFMAN, D.A., "Remote home health care technologies: How to ensure privacy? Build it in: Privacy by design", *Identity in the Information Society*, Vol. 3, Núm. 2, 2010, p. 369

[556] GT29, Opinión 3/2010 sobre el principio de responsabilidad (WP 173), 13 de julio de 2010, p.17

[557] Para comprender adecuadamente este argumento, podemos utilizar el ejemplo visual de las aplicaciones informáticas. Si una persona que quiere descargarse en su móvil una aplicación que cumpla un determinado fin y, tras acudir a la plataforma de distribución digital de aplicaciones móviles que tiene en su teléfono, encuentra dos posibles aplicaciones pero solo una de ellas tiene el certificado que manifiesta el cumplimiento del artículo 25 del RGPD, tendrá la certeza de que al utilizar esa aplicación se respetará en todo momento su derecho a la protección de datos personales, hecho que no puede prometer la restante aplicación.

[558] DE LA MATA BARRANCO, N.J. y BARINAS UBIÑAS, D., "La privacidad en el diseño y el diseño de la privacidad, también desde el derecho penal", *Eguzkilore*, Núm. 28, 2014, p. 263

7. EL CONSENTIMIENTO DE LA PERSONA MAYOR CON DISCAPACIDAD TRAS LA ENTRADA EN VIGOR DE LA LEY 8/2021:

Tras analizar en el capítulo segundo el efecto que ha tenido la reforma en la capacidad de la persona mayor con discapacidad, debemos aplicar la misma lógica al consentimiento del interesado que otorga la persona mayor con discapacidad en el ámbito sanitario, teniendo en cuenta las características que debe reunir todo consentimiento para ser válido, a las que nos hemos referido en los apartados anteriores.

Hemos dicho más arriba que el derecho a la protección de datos personales está íntimamente relacionado con la autonomía del interesado, puesto que persigue garantizarle poder de control sobre sus datos personales, sobre su uso y destino. Por ello, en respeto a la autonomía y voluntad del interesado, solo se realizarán los tratamientos que autorice este último, exceptuando los casos que se recogen en las leyes aplicables.

No hay duda de que las personas mayores son merecedoras del disfrute del derecho fundamental a la protección de sus datos personales en condiciones de igualdad sustantiva, real y efectiva al resto de los ciudadanos, significando la privación o menoscabo del mismo un trato discriminatorio y contrario a su propia dignidad personal[559].

Es decir, el derecho a la protección de datos personales es un derecho que poseen todas las personas tengan o no una discapacidad tanto física como mental, por ello, se ha de superar la tendencia histórica de convertir a las personas mayores con discapacidad en un ser sin voz ni voto, y esto también es aplicable al ámbito de su derecho a la protección de datos. Frente a estas afirmaciones observamos que a menudo las personas mayores son objeto de una protección paternalista alejada del reconocimiento de la autonomía plena de la voluntad que debe reconocérseles. Dichos patrones pueden producirse asimismo en relación al consentimiento de las personas mayores sobre el tratamiento de sus datos, abocando a un escenario donde su voluntad no sea tenida en cuenta.

Frente a esta realidad extendida, no solo en la práctica sino también en el seno de la propia normativa europea armonizadora, es preciso recordar que la persona con discapacidad tan solo precisa de alguien que le ayude a comprender la decisión a adoptar y su trascendencia, a superar sus miedos y dudas injustificadas. Para ello necesita una persona de apoyo, un compañero de camino, que no tome decisiones "por" la persona sino "con" ella[560]. Por consiguiente, pese a tratarse de un sujeto frágil, es preciso contar con su propia voluntad[561].

---

[559] GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M., "La protección de datos de las personas mayores, necesidad y reto para una innovación tecnológica de calidad", *cit.*, p. 586

[560] VIVAS-TESÓN, I., "Discapacidad y consentimiento informado en materia de tratamientos sanitarios y de bioinvestigación", *Civilistica. com*, Vol. 3, Núm. 2, 2014, p. 26

[561] VIVAS-TESÓN, I., "Discapacidad y consentimiento informado en el ámbito sanitario y bioinvestigador", *Pensar-Revista de Ciências Jurídicas*, Vol. 21, Núm. 2, 2016, pp. 537-538

Recuérdese que, de acuerdo con la nueva regulación de la discapacidad, la titularidad de la decisión recae en la propia persona con discapacidad, los apoyos para el otorgamiento del consentimiento del interesado deben estar disponibles para que la persona con discapacidad que lo necesite pueda contar con la asistencia necesaria que la iguale en condiciones con los demás. Por otra parte, la información debe estar disponible en todos aquellos formatos alternativos que requiera la persona con discapacidad. En cuanto a la accesibilidad[562], se ha de optar por la información por capas, y el uso de un lenguaje sencillo, a lo que se le ha de sumar la necesidad de ofrecer la información en formatos adecuados, siguiendo las reglas marcadas por el principio del diseño para todos, de manera que resulten accesibles y comprensibles a las personas con discapacidad, para favorecer que puedan prestar por sí mismas su consentimiento[563]. En toda norma en la que se regule el consentimiento para un determinado acto se debe contemplar que tanto la información previa como el proceso de prestación del consentimiento sean no solo accesibles, sino también comprensibles[564].

El ejercicio de este apoyo siempre debe estar unido al respeto de la voluntad, intereses y preferencias del interesado. Como, en base al artículo 255 de la Ley 8/2021, cualquier persona mayor de edad en previsión o apreciación de la concurrencia de circunstancias que puedan dificultarle el ejercicio de su capacidad jurídica en igualdad de condiciones con las demás, puede prever o acordar en escritura pública medidas de apoyo relativas a su persona o bienes. En el caso de que no exista una voluntad manifiesta, se deberá realizar la mejor interpretación posible de la voluntad y preferencias.

En este sentido, VIVAS-TESÓN recalca tanto el valor del testamento vital, como de la escritura de autotutela, hoy en día autocuratela, puesto que permiten planificar y decidir *pro futuro* la vida propia evitando que lo hagan terceros ante situaciones en las cuales ya nos será posible manifestar dicha voluntad[565]. Y para el caso de que no exista ninguno de los instrumentos citados, la falta de información no legitima una actuación basada en lo que se considera mejor o más conveniente para la persona con discapacidad desde la óptica del intérprete de la voluntad, sino una actuación basada en lo que la persona con discapacidad hubiere preferido o deseado si hubiere podido manifestar su voluntad al respecto[566]. Para ello, se deberá tener en cuenta la trayectoria vital de la persona con discapacidad, sus creencias y valores, así como los factores que ella hubiera tomado en

[562] DE RADA ECHEVARRÍA, M.T., "El consentimiento para la vacuna covid de las personas vulnerables", *OTROSÍ.: Revista del Colegio de Abogados de Madrid*, Núm. 8, 2021, p. 53

[563] PALACIOS GONZÁLEZ, D., "Guarda de hecho, curatela o defesor judicial: Buscando el mejor apoyo para las personas con discapacidad psíquica", en CERDEIRA BRAVO DE MANSILLA, G.; GARCÍA MAYO, M.; GIL MEMBRADO, C. y PRETEL SERRANO, J.J., *Un nuevo orden jurídico para las personas con discapacidad*, Wolters Kluwer, Madrid, 2021, p. 429

[564] VIVAS-TESÓN, I., "Autodeterminación informativa, validez del consentimiento y protección de datos sensibles: críticas al nuevo marco normativo", *Revista de Derecho y genoma humano*, Núm. Extraordinario, 2019, p.265

[565] VIVAS-TESÓN, I., "El consentimiento del adulto frágil al tratamiento de muestras biológicas y datos genéticos con fines de investigación biomédica: comparación entre el derecho español e italiano. Revista de derecho y genoma humano", Núm. 40, 2014, p. 113

[566] GUILARTE MARTÍN-CALERO, C., *El derecho a la vida familiar de las personas con discapacidad: El Derecho español a la luz del artículo 23 de la Convención de Nueva York*, Reus, Madrid, 2021, pp.27-28

consideración, con el fin de tomar la decisión que habría adoptado la persona en caso de no requerir representación.

Se entiende que estas medidas de apoyo voluntarias también pueden referirse al ámbito de protección de datos personales (por tratarse de un derecho de la personalidad), y más concretamente, al ámbito de protección de datos personales en el campo de la salud. Mediante la posibilidad que tiene la persona interesada de diseñar libremente su apoyo (delimitando el régimen de su actuación, el alcance de las facultades de la persona o de las personas que le prestarán el apoyo, y la forma en que se procurará el apoyo, así como las medidas u órganos de control), se pretende garantizar que en el futuro se respete en todo momento su voluntad, deseos y preferencias.

En consecuencia, la persona interesada puede indicar en escritura pública que el apoyo se otorgue en el ámbito de la protección de datos, delimitando el régimen de actuación de la persona física o jurídica que le prestará el apoyo y las medidas de seguridad que considere adecuadas. A su vez, podrá realizar un listado que refleje su voluntad, deseos y preferencias para el caso de que en un futuro no pudiese expresar dicha voluntad, indicando, por ejemplo, si ante una enfermedad como el Alzheimer desea ser geolocalizada o monitorizada o si quiere que sus datos relativos a la salud sean utilizados para la investigación sanitaria. En el ámbito de la salud son de uso común las instrucciones previas[567] y las voluntades anticipadas[568], pero en el caso del derecho a la protección de datos no ha existido hasta el momento ningún instrumento que posibilitara plasmar anticipadamente la voluntad del interesado. Esta carencia ha estado muy condicionada a la poca conciencia que existe en relación a este derecho fundamental y que los conceptos del consentimiento informado e interesado sean entendidos erróneamente como sinónimos.

La persona que preste el apoyo, deberá acompañar a la persona con discapacidad para que esta pueda otorgar su consentimiento tras ser debidamente informada, siempre teniendo en cuenta la accesibilidad de la información. Uno de los graves problemas es controlar que realmente es la voluntad de la persona mayor con discapacidad otorgar el consentimiento del interesado para el tratamiento de sus datos relativos a la salud. En el caso de los proyectos de investigación, es más fácil que el médico en cuestión vea que la persona con discapacidad, tras ser debidamente informada y con el apoyo que requiera, sea quien otorgue su consentimiento del interesado libremente. Pero esta

[567] Según recoge el artículo 11 de la LBAP *"por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo. El otorgante del documento puede designar, además, un representante para que, llegado el caso, sirva como interlocutor suyo con el médico o el equipo sanitario para procurar el cumplimiento de las instrucciones previas".*

[568] Según el artículo 2.1 de la Ley 7/2002, de 12 de diciembre de 2002, de las voluntades anticipadas en el ámbito de la sanidad "*cualquier persona mayor de edad que no haya sido judicialmente incapacitada para ello y actúe libremente tiene derecho a manifestar sus objetivos vitales y valores personales, así como las instrucciones sobre su tratamiento, que el médico o el equipo sanitario que le atiendan respetarán cuando se encuentre en una situación en la que no le sea posible expresar su voluntad*".

verificación se dificulta claramente en el caso de las aplicaciones móviles, puesto que no existe forma alguna de comprobar quien ha descargado realmente la aplicación, y otorgado el consentimiento para que se realice el tratamiento de los datos personales. Esto es, actualmente no es posible controlar si es el mismo interesado o una tercera persona quien otorga el consentimiento en el particular ámbito de las aplicaciones móviles, lo cual puede poner en peligro el derecho a la protección de datos personales de las personas mayores con discapacidad.

Las medidas de provisión de apoyos de carácter judicial son, como sabemos, subsidiarias a las de carácter voluntario previstas por la propia persona con necesidad de ellas, así como a los apoyos de hecho si vienen resultando eficaces, pero lo que es más importante, la provisión de un apoyo representativo es excepcional, tanto si es puntual como si es de carácter estable y formal[569]. Cuando, pese a haberse hecho un esfuerzo considerable, no sea posible determinar la voluntad, deseos y preferencias de la persona, las medidas de apoyo podrán incluir funciones representativas. En el caso de que se deba otorgar un consentimiento por representación, por ejemplo mediante curatela representativa, este acto deberá realizarse valorando en todo momento qué hubiera querido el interesado en caso de poder decidir por sí mismo[570].

La autonomía individual, la independencia y la libertad para tomar decisiones deben ser limitadas para lo estrictamente necesario, a fin de que la persona con discapacidad pueda adoptar sus decisiones en las mismas condiciones que las demás personas. No se le puede otorgar más apoyo del que necesita, puesto que se vulnerarían los principios de proporcionalidad y autonomía, ni menos, dado que se vulnerarían los principios de necesidad, proporcionalidad y no discriminación, al colocarla en una situación de desventaja respecto de las demás personas[571].

El RGPD no habla en ningún momento de representantes legales en su artículo 9.2.a), y se refiere exclusivamente al consentimiento explícito del interesado como una de las bases legales para el tratamiento de sus datos relativos a la salud[572]. Solo se diferencia el

[569] GONZÁLEZ CARRASCO, C., "La prestación del consentimiento informado en materia de salud en el nuevo sistema de apoyos al ejercicio de la capacidad", *Derecho privado y Constitución*, Núm. 39, 2021, pp. 229-230

[570] En este sentido, previa a la reforma, ALKORTA IDIAKEZ afirmaba que la posibilidad de otorgar el consentimiento mediante representación podía crear un potencial conflicto de intereses entre las personas discapacitadas y sus representantes legales puesto que, a menudo, las personas cuidadoras y los representantes legales de las personas mayores son las mismas, y podían tener interés en monitorizar las constantes vitales y los movimientos de las personas mayores que representaran para recibir, entre otras cuestiones, avisos de su estado de salud. Sin embargo, según alegaba, los representantes debían velar por los intereses de sus representados, procurando respetar sus valores, es decir, poniéndose en su lugar a la hora de consentir el tratamiento de datos sanitarios mediante dispositivos conectados. Véase al respecto: ALKORTA IDIAKEZ, I., "La protección del derecho a la autodeterminación informativa de los mayores en entornos conectados" en ALKORTA IDIAKEZ, I. y ATIENZA MACÍAS, E., *Soluciones tecnológicas para los problemas ligados al envejecimiento. Reglamento General de Protección de Datos. Hacia un nuevo* modelo de Privacidad, Dykinson, Madrid, 2020, pp.50-51

[571] GUILARTE MARTÍN-CALERO, C., *Comentarios a la Ley 8/2021 por la que se reforma la legislación civil y procesal en materia de discapacidad*, Aranzadi, Pamplona, 2021, pp. 685-686

[572] No obstante, el artículo 49.1. f) del RGPD habla de la situación en la que "el interesado esté física o jurídicamente incapacitado para dar su consentimiento", cuestión que es contraria a la reforma.

consentimiento del menor, que, según el artículo 8.1 del RGPD, si el niño es menor de 16 años, el tratamiento únicamente se considerará lícito cuando el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. En el caso de España, el artículo 7.1 de la LOPDGDD recoge que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años. El tratamiento de los datos de los menores de catorce años, fundado en el consentimiento, solo será lícito si consta el consentimiento del titular de la patria potestad o tutela.

Igualmente, a nivel estatal, se ha de comprender que aunque solo se hable del "afectado", en los casos en los que exista una discapacidad, será el mismo interesado con discapacidad con el apoyo que necesite quien otorgará el consentimiento del interesado[573]. En el caso de que se deba dar un consentimiento por representación por parte del curador representativo, este acto se deberá llevar a cabo valorando en todo momento la voluntad, deseos y preferencias del interesado.

Si el tratamiento de los datos relativos a la salud va en contra de la voluntad del interesado, ya sea porque lo haya expresado el mismo o se haya interpretado de esta manera, la única forma de realizar dicho tratamiento será justificarlo en otra base legal del artículo 9.2 del RGPD. En este sentido, es de interés citar el informe 0292/2010, de 18 de octubre de 2012 de la AEPD, en el cual se analizaba una consulta sobre la comercialización y utilización de microchips intradérmicos (implantados en el usuario) mediante los que se podría incorporar información referente a sus portadores. La AEPD indicó que "*la información del dispositivo o la señal emitida por el mismo, en su caso, debería ser objeto de procedimientos que impidiesen lecturas no permitidas por el interesado, o su representante legal cuando se tratase de un incapacitado (lo que resulta aplicable al caso, dado que la consulta hace referencia a la localización de enfermos de Alzheimer). Ello implica la necesaria implantación en el propio dispositivo de medidas que garantizasen el cifrado de toda la información o de la señal contenida en el chip para evitar su lectura en supuestos en los que no concurra el consentimiento del interesado*".

Dado que se trata de un informe emitido antes de la entrada en vigor de la nueva Ley 8/2021, se ha de realizar una interpretación adaptada en la que la figura del representante legal es sustituida por la persona que otorga el apoyo. Una vez aclarado este punto, y en base a todo lo antedicho, debe alegarse que la implantación de estos microchips intradérmicos y el tratamiento de los datos personales que se realice mediante su uso, no puede realizarse en contra de la voluntad del interesado. La persona que otorgue el apoyo no podrá permitir el tratamiento de los datos personales en contra de la voluntad de la persona mayor con discapacidad. En el caso de que se trate de un apoyo representativo, y no exista una voluntad expresa del interesado, la persona que otorgue el apoyo representativo tendrá la obligación de realizar la mejor interpretación posible de la voluntad y preferencias del mismo. Cuando, aun habiendo realizado la

[573] El artículo 6 de la LOPDGDD solo habla del "consentimiento del afectado" y el artículo 9.1 de la misma norma se refiere al artículo 9.2 del RGPD.

interpretación no sea posible saber el deseo del interesado, como norma general, no se podrá realizar el tratamiento de los datos personales.

Esta afirmación es extensible al uso de los dispositivos tecnológicos llevables que monitoricen las constantes vitales y/o geolocalicen al interesado mayor con discapacidad. No es cierto que este tratamiento fomentaría su autonomía permitiendo un envejecimiento activo y saludable, puesto que se estaría controlando cada paso que da, convirtiendo su vida en un *reality*. Las nuevas tecnologías pueden ser unas aliadas para las personas mayores con discapacidad, pero también pueden constituir una amenaza para su intimidad y su autonomía cuando son aplicadas en contra de su voluntad. En consecuencia, cuando no exista esta voluntad, el acompañamiento humano no debe ser sustituido por el avance tecnológico. La geolocalización puede ser evitada con el acompañamiento de una persona. El reforzamiento de las ayudas sociales para este sector poblacional, permitiría rehuir la geolocalización y, a su vez, proteger el derecho a la protección de datos de las personas mayores.

Por otra parte, aunque el interesado haya expresado su negativa a que se realice un determinado tratamiento de sus datos personales en el futuro, esta voluntad no impide la recolección y análisis de datos realizado gracias a otra base legal. El problema será justificar adecuadamente el uso de esa otra base legal, puesto que se estaría limitando el control del interesado sobre sus datos personales. El tratamiento que se realice de acuerdo con otra base legal, deberá respetar los principios del RGPD, en especial, el principio de minimización de datos, el principio de limitación del plazo de conservación y el principio de integridad y confidencialidad. Así, si se puede justificar un tratamiento de datos personales en contra de la voluntad de la persona mayor con discapacidad por aplicación de otra base legal, solo se podrán recolectar y analizar los datos que sean necesarios, la conservación de esos datos estará limitada en el tiempo al logro de los fines que persigue el tratamiento, y se introducirán las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos.

Es posible que un futuro el uso de los objetos inteligentes esté tan normalizado como el uso de un marcapasos en la asistencia sanitaria, por ello, el tratamiento de los datos relativos a la salud que realizarían podría basarse en el artículo 9.2.h) del RGPD[574]. No obstante, dicho tratamiento tendría que respetar los principios del RGPD, no pudiendo recolectar ni analizar los datos personales del interesado las 24 horas del día, y debiendo introducir medidas técnicas y organizativas para garantizar la integridad, la disponibilidad y la confidencialidad de los datos. En otras palabras, cabe la posibilidad de que, en un futuro no muy lejano, los objetos inteligentes sean un elemento inseparable de la asistencia sanitaria, pudiendo legitimar el tratamiento de los datos

[574] Artículo 9.2.h) del RGPD: "*el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3"*.

personales en la citada base legal. Sin perjuicio de lo anterior, este tratamiento deberá cumplir todos los principios que se recogen en el artículo 5 del RGPD.

En cuanto al segundo caso, cuando no exista una voluntad expresa del interesado, se deberá realizar la mejor interpretación posible de la voluntad y preferencias del mismo. En el caso particular de que, aun habiendo realizado la interpretación no se pueda deducir el deseo del interesado, como norma general, no se podrá realizar el tratamiento de los datos relativos a la salud salvo que se pueda justificarlo en otra base legal. Para poder llevar a cabo un tratamiento de datos relativos a la salud de la persona mayor con discapacidad, tendremos que averiguar si este lo otorga, ya sea con el apoyo que necesita o, en los casos más extremos, por representación tras una previa manifestación del mismo ante notario o interpretación de su voluntad. Cuando no exista este consentimiento, también aplicable al caso en el que aun habiendo realizado la interpretación no se pueda deducir el deseo del interesado, se deberá analizar si puede ser de aplicación otra base legal del artículo 9.2 del RGPD, como por ejemplo el ya citado artículo 9.2.h) del RGPD, lo cual convertiría el tratamiento en lícito.

Otra cuestión sería saber si el concepto de interés superior[575] tiene cabida en el ámbito de la protección de datos personales, y en caso de que así sea, cuándo ha de ser aplicada. Tal y como se ha indicado anteriormente, la reforma aboga por la voluntad de la persona mayor con discapacidad[576], a su vez, el concepto del interés superior es únicamente

[575] Ya en el Punto 21 de la Observación general Nº 1 del 2014 del CRPD se recogía que, cuando, pese a haberse hecho un esfuerzo considerable, no sea posible determinar la voluntad y las preferencias de una persona, la determinación del interés superior debe ser sustituida por la mejor interpretación posible de la voluntad y las preferencias; puesto que así se respetan los derechos, la voluntad y las preferencias de la persona de conformidad con el artículo 12.4 de la Convención. El principio del "interés superior" no es una salvaguardia que cumpla con el artículo 12 en relación con los adultos. El paradigma de "la voluntad y las preferencias" debe reemplazar al del "interés superior" para que las personas con discapacidad disfruten del derecho a la capacidad jurídica en condiciones de igualdad con los demás.

[576] Al hilo del necesario respeto a la voluntad, deseos y preferencias de la persona con discapacidad, GARCÍA RUBIO hace una reflexión sobre la obligatoriedad de vacunar contra el virus del COVID-19 a las personas mayores internadas en centros geriátricos o de otro tipo, poniendo claramente de relieve la contraposición entre las decisiones tomadas con base en la voluntad de la persona con discapacidad y las adoptadas según su mejor interés, criterio descartado por la Convención. Para realizar este ejercicio, la autora analiza las sentencias SPI núm. 6 de Santiago de Compostela de 20 de enero de 2021, SPI núm. 8 de Alicante de 8 de febrero de 2021 y SPI núm. 4 de Lugo de 11 de febrero de 2021, que en contra de los familiares encargados de otorgar el consentimiento informado, y en base al mejor interés, obligaban a vacunar a las personas internadas.

En palabras de la autora, si la persona está en condiciones de dar su consentimiento por sí sola, este ha de ser el único criterio a seguir. Si para formar y declarar una opinión la persona precisa de apoyos o adaptaciones tanto en el proceso de información médica como en el de expresión de su voluntad, deberán proporcionarse unos y otros. Por último, en el caso de que no pueda expresar su voluntad, se deberá averiguar la voluntad, deseos y preferencias de la persona mayor, incluso acudiendo a su trayectoria vital, comprobando, por ejemplo, si con anterioridad se ha puesto o no voluntariamente otras vacunas. Por ello, el único motivo que podía conducir a una resolución que impusiera la vacunación prescindiendo o contrariando el criterio de la persona afectada era que razones de salud pública hicieran aconsejable que todos los internos recibieran la vacuna. Esto sucedería si la vacuna fuera obligatoria para todos los ciudadanos o para determinados colectivos como internos de una residencia de ancianos debido a su especial vulnerabilidad al contagio y los especiales riesgos para su salud y su vida, incluso contra su voluntad, cosa que no se ha impuesto en la realidad. Véase al respecto: GARCÍA RUBIO, M.P., "La reforma de la discapacidad en el Código Civil. Su incidencia en las personas de edad Avanzada", *cit.*, pp. 90-91; En el mismo sentido: Auto del Juzgado de Primera Instancia número 16 de Granada de 4 de

mencionado en el artículo 92 de la LOPDGDDD sobre la protección de datos de los menores en internet, y no se utiliza en ningún otro contexto en la normativa. No obstante, el consentimiento del interesado, aun siendo tradicionalmente la base legal más utilizada, es solamente una de las vías que legitima el tratamiento de los datos relativos a la salud, por tanto, dicho tratamiento puede justificarse en otra base legal.

Según VIVAS-TESÓN, el principio rector que atraviesa de principio a fin la nueva Ley es el del respeto de la voluntad, deseos y preferencias de la persona con discapacidad, lo que aleja de la visión paternalista que ha caracterizado hasta ahora a la normativa, la cual el legislador considera "periclitada". Por ello, según afirma, no existe el principio del interés superior de la persona con discapacidad, al cual, de manera intencionada, no se menciona ni una sola vez en el nuevo texto legal[577]. Esta interpretación del contenido de la nueva ley elimina el criterio del interés de la persona con discapacidad para basarse únicamente en el respeto de su voluntad, interés y preferencias. Este planteamiento parte de la premisa de que, como regla general, es la persona con discapacidad quien puede decidir cuál es su interés, incluso aunque se equivoque, puesto que tiene el mismo derecho a equivocarse que todas las demás[578].

Conforme a LECIÑENA IBARRA, es normal que las personas intenten experimentar por sí mismas, tomando la decisión más oportuna según su criterio, aunque con ello se equivoquen, como ocurre con las personas que no tengan una discapacidad. El riesgo de cometer un error debe asumirse en un contexto en el que la decisión haya sido tomada de manera consciente, voluntaria y libre por quien la ha manifestado. En este escenario, la persona que ha prestado el apoyo para que la persona con discapacidad haya podido culminar el proceso deliberativo no ostentará poder alguno para vetar tal decisión pues tal actuación supondría una restricción en el ejercicio de su capacidad jurídica, carente de justificación en la norma. La persona con discapacidad es dueña de su decisión, por muy extraña o excéntrica que esta sea, pues lo que se somete a control no es la decisión que ha podido adoptar sino la aptitud que se ha tenido para tomarla[579].

Ante esta lectura, la autora PEREÑA VICENTE indica que, en ciertas ocasiones es imposible conocer la voluntad, deseos y preferencias de la persona que requiere el apoyo, ni siquiera intuir qué decisión sería la más ajustada a sus valores y estilo de vida. Así, según la citada autora, en estos casos, el mejor interés debe operar como segundo

---

febrero de 2021; VIVAS-TESÓN alega que los citados pronunciamientos judiciales se expresan en términos muy similares, quedando lejos del traje a medida que se precisa, y que no consta que en todos los procesos se haya hecho partícipe a la persona del proceso de información y prestación del consentimiento, ni que se haya intentado conocer los deseos de los residentes. Por ello, según indica, si en el momento de resolución hubiera estado ya vigente la Ley 8/2021, los autos contravendrían su espíritu. Véase al respecto: VIVAS-TESÓN, I., *Vivir con discapacidad en el contexto de una pandemia: el derecho a tener derechos*, Tecnos, Madrid, 2021, pp. 193-194

[577] VIVAS TESÓN, I., "La reforma civil y procesal para el apoyo de las personas con discapacidad: ¿A partir de septiembre, qué?", *cit.*

[578] CUENCA GÓMEZ, P., "Reflexiones sobre el Anteproyecto de reforma de la legislación civil española en materia de capacidad jurídica de las personas con discapacidad", *Indret*, Núm. 2, 2020, p.126

[579] LECIÑENA IBARRA, A., "Reflexiones sobre la formación de la voluntad negocial en personas que precisan apoyos en el ejercicio de su capacidad jurídica", *Revista de Derecho Civil*, Vol. 9, Núm. 1, 2022, pp. 282-283

criterio[580]. Deberá ser la jurisprudencia quien establezca cómo ha de interpretarse esta cuestión, y cuando se crea realmente esa imposibilidad de conocer la voluntad, deseos y preferencias de la persona[581]. En el mismo sentido, PAU PEDRÓN indica que, en la contraposición de los criterios del "interés" y la "voluntad", hay que dar preferencia a esta última, y que solo cuando la voluntad no puede expresarse ni reconstruirse entrará en juego el criterio del interés[582]. PEREÑA VICENTE señala que el interés superior ha de prevalecer como criterio moderador o límite de la voluntad claramente manifestada, cuando esta genera un grave perjuicio a la persona, ya sea patrimonial o personal, aunque la dificultad reside en saber cuáles son esos límites[583].

Realizando una interpretación extensiva en la línea apuntada por PAU PEDRÓN creemos que la única forma en la que podría aplicarse el concepto de interés superior es que no se sepa cuál es la voluntad del interesado, no se logre justificar el tratamiento en las restantes bases legales, y que dicho tratamiento sea vital para el bienestar del interesado mayor con discapacidad. Esto vendría a traducirse en que, un determinado tratamiento de datos relativos a la salud es indispensable para la vida y bienestar de la persona mayor con discapacidad. Por ello, si no es indispensable, el tratamiento de los datos relativos a la salud no estará justificado.

En suma, en nuestra opinión, el beneficio de las nuevas tecnologías en el ámbito de la sanidad es indiscutible, pero ello no justifica que se apliquen, en cualquier caso, a cualquier persona y a cualquier nivel. Al igual que no todo vale en nombre de la investigación en salud, no todo vale en nombre del supuesto beneficio para la salud de las personas mayores con discapacidad, sino que debe existir un equilibrio entre los bienes jurídicos contendientes.

[580] En este aspecto TORTAJADA CHARTÍ manifiesta que se debe interpretar y dar preferencia a la voluntad deseos y preferencias de la persona con discapacidad, pero que no debe caerse en el desconocimiento de los diversos niveles de discapacidad, puesto que existen situaciones en que no será posible conocer la voluntad de la persona o ésta sea contradictoria, o incluso perjudicial para ella misma, ejerciendo por tanto la medida de apoyo en detrimento del interés superior de la persona con discapacidad. Véase: TORTAJADA CHARTÍ, P., "La patria potestad prorrogada y la patria potestad rehabilitada en el nuevo proyecto de Ley de reformas de la legislación civil y procesal para el apoyo a las personas con discapacidad (actual Ley 8/2021)", *cit.*, p. 247

[581] PEREÑA VICENTE, M., *La protección jurídica de adultos: el estándar de intervención y el estándar de actuación: entre el interés y la voluntad*, Dykinson, 2018, p. 140

[582] PAU PEDRÓN, A., "De la incapacitación al apoyo: el nuevo régimen de la discapacidad intelectual en el Código Civil", *Revista de Derecho Civil*, Vol. 5, Núm. 3, 2018, p. 9

[583] PEREÑA VICENTE, M., *La protección jurídica de adultos: el estándar de intervención y el estándar de actuación: entre el interés y la voluntad*, p. 139

CAPÍTULO 4: LA INVESTIGACIÓN EN SALUD EN EL RGPD Y EN LA NORMATIVA ESPAÑOLA, ITALIANA E IRLANDESA

1. INTRODUCCIÓN:

El tratamiento de los datos relativos a la salud con fines de investigación tiene un gran valor, permitiendo, entre otras cuestiones, realizar unos diagnósticos más exactos, crear nuevos medicamentos y planificar estrategias de salud pública. Aunque el uso de los datos relativos a la salud para la investigación sea fundamental para la renovación tecnológica en la que está inmerso el sector, este ejercicio debe realizarse con las máximas garantías para los derechos de los interesados. Es decir, ha de existir un equilibrio entre el uso de los datos para la investigación científica y la salvaguarda del derecho fundamental a la protección de datos personales.

Aunque el RGPD prometía armonizar el uso de datos relativos a la salud para la investigación sanitaria a nivel europeo, finalmente renunció a ello reconociendo en su artículo 9.4 a los Estados miembros la posibilidad de mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de los datos relativos a la salud. El legislador español ha desarrollado dicha remisión a través de la Disposición Adicional Decimoséptima de la LOPDGDD. Pero existen también otros ordenamientos estatales de referencia que interesa analizar debido a las diferencias que se aprecian entre las mismas, lo cual refleja claramente la falta de armonización en el ámbito de la investigación sanitaria. Con el objetivo de remarcar estas divergencias, se ha optado por analizar la normativa italiana e irlandesa, por comprender notables disimilitudes en cuanto al ordenamiento estatal. En cuanto a Italia, el tratamiento de datos relativos a la salud con fines de investigación se regula en el capítulo VII de su Decreto legislativo 196/2003 de 30 de junio de 2003, el cual ha sido reformado por el Decreto legislativo 101/2018 de 10 de agosto. Por su parte, Irlanda ha optado por regular la presente materia específicamente en su Ley 314/2018 de Protección de Datos (Sección 36(2) Investigación en Salud), la cual entró en vigor el 8 de agosto de 2018.

Por otra parte, la pandemia provocada por el COVID-19 ha puesto de relieve el papel que desempeña la recopilación y el análisis de datos clínicos para avanzar en la investigación científica, y así combatir el virus. No obstante, también ha quedado patente que las salvaguardas de protección de datos son esenciales para generar confianza pública, debiendo, nuevamente, encontrar un equilibrio entre el derecho fundamental a la protección de datos personales y la investigación científica. Los distintos países europeos han estado desarrollando múltiples estrategias encaminadas a la minería de datos para confrontar la pandemia[584]. Con este fin, se han apoyado en

[584] El "Green Pass" o certificado digital verde ha suscitado numerosas opiniones entre los autores[584], puesto que el mismo ha constituido un tratamiento datos relativos a la salud[584]. El objetivo de este certificado ha sido permitir el ejercicio del derecho a la libre circulación dentro de la UE durante la pandemia de COVID-19 mediante el establecimiento de un marco común aplicable a la expedición, verificación y aceptación de certificados interoperables de vacunación, pruebas y recuperación de la COVID-19, tratando para ello los datos relativos a la salud de los interesados. Por ende, es necesario

distintas bases legitimadoras que serán analizadas en el presente capítulo, siendo diferente el tratamiento de los datos relativos a la salud con fines de investigación que se ha realizado en el ámbito de la pandemia por ejemplo en España, Italia o Irlanda.

De este modo, en este apartado se analizarán las bases legitimadoras para el tratamiento de los datos relativos a la salud para la investigación sanitaria del RGPD, de la Ley Orgánica española, del Código italiano y de la ley irlandesa; y se expondrá de qué manera se ha hecho uso de las mismas en el contexto de la pandemia. Todo ello pondrá de manifiesto los problemas que, desde la perspectiva del derecho a la protección de datos personales, plantea la falta de una legislación armonizada en el campo de la investigación sanitaria nacional e internacional. A su vez, debido a la entrada en vigor de la Ley 8/2021 que ha sido analizada en el capítulo 2 del presente trabajo, es necesario realizar una nueva lectura de la base legitimadora del consentimiento que se recoge en la Disposición Adicional Decimoséptima de la LOPDGDD para la investigación en salud y el caso de las personas mayores con discapacidad. Tras el análisis del RGPD y las tres seleccionadas normativas, se llevará a cabo una comparación entre estas tres últimas, acción que permitirá efectuar ciertas propuestas encaminadas a uniformar la presente materia a nivel europeo.

Por último, en el contexto de la creación del Espacio Europeo de Datos Sanitarios (EEDS), y la entrada en vigor del Reglamento 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022 relativo a la gobernanza de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)[585], se estudiará brevemente el concepto del formulario europeo de consentimiento para la cesión altruista de datos que se prevé en la citada norma como una oportunidad para introducir criterios comunes, y tratar de armonizar el consentimiento del interesado para el tratamiento de sus datos personales con fines de investigación a nivel europeo.

---

contar con una base legal apropiada para realizar dicho tratamiento de datos personales y establecer las salvaguardas adecuadas[584]. Sin perjuicio de lo anterior, dado que el objetivo del presente capítulo es analizar las bases legitimadoras para el tratamiento de datos relativos a la salud para la investigación sanitaria, y el fin del tratamiento de datos personales que se realiza con el Green Pass es el control (controlar que el interesado ha sido vacunado, que ha recibido un resultado negativo de una prueba diagnóstica o se ha recuperado de esa enfermedad), y no la investigación, no se realizará un análisis jurídico del certificado, dejando dicha labor para futuras investigaciones. Véanse al respecto: ARENAS RAMIRO, M., "Pasaporte Covid, ¿libertad de circulación de forma segura o discriminación y privacidad en juego?", *La Ley privacidad*, Núm.8, 2021; WAITZBERG, R.; TRIKI, N.; ALROY-PREIS, S.; LOTAN, T.; SHIRAN, L. y ASH, N., "The Israeli Experience with the "Green Pass" Policy Highlights Issues to Be Considered by Policymakers in Other Countries", *International Journal of Environmental Research and Public Health*, Vol. 18, Núm. 21, 2021; RONCATI, L. y RONCATI, M., "COVID-19 Green Pass: a Lesson on the Proportionality Principle from Galicia", *European Journal of Health Law*, Núm. 1, 2021, pp.1-8; GRASSELLI, F. y TEVERE, V., "Il green pass esteso nello spazio europeo multilevel di libertà, sicurezza e giustizia. Riglessioni sull´eventuale introduzione dell´obbligatorietà vaccinale", *Freedom, Sevurity & Justice: European Legal Studies*, Núm.3, 2021; COMISIÓN EUROPEA. "Preguntas y respuestas: Certificado COVID digital de la UE", *ec.europa.eu*, 1 de junio de 2021, disponible en: https://ec.europa.eu/commission/presscorner/detail/es/QANDA_21_2781 *[Última consulta: 25 de julio de 2021];* CEPD., "Las autoridades de protección de datos de la UE adoptan un dictamen conjunto sobre las propuestas de certificado digital verde", *edpb*, 6 de abril de 2021, disponible en: https://edpb.europa.eu/news/news/2021/eu-data-protection-authorities-adopt-joint-opinion-digital-green-certificate_es *[Última consulta: 25 de julio de 2021]*

[585] DOUE núm. 152, de 3 de junio de 2022

Aunque es cierto que dentro del nuevo Reglamento 2022/868 se identifican otras vías distintas a la presente para realizar el tratamiento de los datos relativos a la salud, debido a que uno de los principales fines de este trabajo es el análisis de la figura del consentimiento del interesado y, sobre todo, el consentimiento del interesado que otorga la persona mayor con discapacidad, el análisis de estas distintas herramientas o vías se dejará para futuros trabajos de investigación.

2. DELIMITACIÓN DE LOS CONCEPTOS:

Antes de profundizar en el presente tema, es necesario delimitar los conceptos de "tratamiento" e "investigación científica" para comprender realmente a que se refieren los mismos y así, una vez definido el campo de estudio de este capítulo, adentrarse en el análisis de los apartados que lo constituyen.

Tal y como se ha indicado anteriormente, se comprende por tratamiento cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción[586]. Este término comprende el tratamiento automatizado (realizado con ayuda, por ejemplo, de un ordenador o un dispositivo móvil) y no automatizado[587] (manual) de los datos personales[588]. Así, cualquier operación realizada con datos personales será comprendida como tratamiento.

En cuanto a la investigación científica, a diferencia del anterior término, este concepto no está definido expresamente en el RGPD. Sin embargo, el Considerando 159 del RGDP señala que el tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del RGPD de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, el citado Considerando indica que en base al artículo 179.1 del TFUE, se debe tener en cuenta el objetivo de la Unión de realizar un espacio europeo de investigación[589].

---

[586] Artículo 4.2 del RGPD

[587] La introducción del tratamiento no automatizado dentro del concepto de tratamiento se justifica en el Considerando 15 del RGPD, indicando que a fin de evitar que haya un grave riesgo de elusión, la protección de las personas físicas debe ser tecnológicamente neutra y no debe depender de las técnicas utilizadas. La protección de las personas físicas debe aplicarse al tratamiento automatizado de datos personales, así como a su tratamiento manual, cuando los datos personales figuren en un fichero o estén destinados a ser incluidos en él. Los ficheros o conjuntos de ficheros, así como sus portadas, que no estén estructurados con arreglo a criterios específicos, no deben entrar en el ámbito de aplicación del Reglamento.

[588] CdE. *Manual de legislación europea de protección de datos, cit.*, pp.111-115

[589] Mediante esta referencia expresa al artículo 179.1 del TFUE puede interpretarse que la norma exige, tanto a la investigación pública como a la privada, que se pueda acceder al resultado de la investigación a través de la publicación o de otro medio que garantice la libre circulación de los conocimientos científicos y tecnológicos. No obstante, las normas éticas de la investigación y de su publicación carecen de un marco normativo armonizado a nivel europeo, y el RGPD tampoco especifica dichas pautas. La falta de

El RGPD consolida una concepción amplia de la investigación que, pese a no definirse expresamente, incluye el desarrollo tecnológico, la demostración, la investigación fundamental, la investigación aplicada e incluso la investigación financiada por el sector privado[590]. Se trata de una enumeración "*numerus apertus"* en la que deben incluirse, entre otros, la investigación biomédica y la investigación trasnacional. No obstante, el GT29 considera que la noción no debe ampliarse más allá de su significado común, y entiende que la investigación científica en este contexto se refiere a un proyecto de investigación establecido con arreglo a las correspondientes normas metodológicas y éticas relacionadas con el sector, de conformidad con prácticas adecuadas[591].

Se diferencia la investigación "científica" de la "histórica" y de los "fines estadísticos", y abarca tanto la investigación en las ciencias de la vida como en otros campos, por ejemplo, las ciencias sociales[592]. La investigación científica debe reportar "beneficios", al menos potencialmente, y esta expectativa justifica un régimen singular que permite establecer excepciones a ciertos derechos[593] tal y como se analizará en el siguiente capítulo[594].

En base a lo antedicho, el tratamiento de los datos personales con fines de investigación científica puede comprenderse como cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales con el objetivo de realizar un análisis o examen científico. Se distinguen dos tipos de uso de datos en lo que respecta al tratamiento de datos relativos a la salud con fines de investigación científica: investigación sobre datos relativos a la salud directamente recopilados con dichos fines ("uso principal"), e investigación sobre datos personales relativos a la salud, que consiste en el procesamiento posterior de los datos recolectados para otro propósito ("uso secundario")[595].

Los datos relativos a la salud constituyen la materia prima para llevar a cabo el tratamiento de los datos personales con fines de investigación en salud. Aunque es cierto que esos datos provienen de los individuos, la investigación no pone en peligro su integridad física, sino su derecho a la protección de datos. Por ende, el elemento de

---

una definición clara dará pie a diversas interpretaciones, debiendo pronunciarse el Comité Europeo de Protección de Datos. Véase al respecto: ALKORTA IDIAKEZ, I., "Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías Bigdata", Revista de derecho y genoma humano, Núm. Extra 1, 2019, p. 298

[590] Considerando 159 del RGPD

[591] CEPD. Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, *cit.*, p. 5

[592] Considerandos 157 y 159 del RGPD

[593] NICOLÁS JIMÉNEZ, P., y TERRIBAS I SALA, N., "Investigación con datos de carácter personal", en ROMEO CASABONA, C.M (Dir.); NICOLÁS JIMÉNEZ, P., y ROMEO MALANDA, S. (Coord.), *Manual de bioderecho (Adaptado para la docencia en ciencias de la salud y ciencias sociales y jurídicas)*, Dykinson, Madrid, 2022, p. 685

[594] Artículo 89.2 del RGPD

[595] HANSEN, J.; WILSON, P.; VERHOEVEN, E.; KRONEMAN, M.; KIRWAN, M.; VERHEIJ, R. y VAN VEEN, E. B., *Assessment of the EU Member States' rules on health data in the light of GDPR*, *cit.*, p. 57

trabajo o componente principal de este tipo de estudios son los datos personales, debiendo poner el foco en su protección.

3. EL TRATAMIENTO DE LOS DATOS RELATIVOS A LA SALUD CON FINES DE INVESTIGACIÓN CIENTÍFICA EN EL RGPD:

En este apartado se analizarán las bases legales que se identifican en el RGPD para el tratamiento de los datos relativos a la salud con fines de investigación científica, con el objetivo de exponer cómo se ha regulado este ámbito a nivel europeo, para más tarde centrarnos en los casos particulares de España, Italia e Irlanda. Tal y como se ha indicado anteriormente, esta comparación permitirá identificar las divergencias normativas que se aprecian entre los distintos países, lo cual refleja la falta de armonización en el ámbito de la investigación sanitaria a nivel europeo. Una vez realizado el análisis de las bases legales del RGPD, en este mismo apartado veremos cómo se han podido utilizar las mismas en el contexto de la pandemia de COVID-19.

3.1. Bases legales:

El artículo 9.2 del RGPD identifica distintas situaciones que permiten realizar el tratamiento de datos relativos a la salud con fines de investigación siembre que el tratamiento sujeto a las garantías adecuadas[596]: cuando el interesado haya otorgado su consentimiento, cuando existan razones de un interés público esencial o interés público en el ámbito de la salud pública, o cuando sea aplicable la excepción de la investigación[597]. En cuanto al consentimiento del interesado, aunque en el anterior capítulo se ha estudiado la base legal del consentimiento del interesado para el tratamiento de los datos relativos a la salud, como se adelantaba, el análisis del concepto no se ha agotado en el citado capítulo. En el presente capítulo se analizará la institución del consentimiento del interesado como base legitimadora del tratamiento de los datos relativos a la salud para el ámbito específico de la investigación científica.

3.1.1. Consentimiento del interesado:

Como se viene exponiendo, el artículo 9.1 del RGPD prohíbe, entre otros, el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física y datos relativos a la salud. Sin perjuicio de lo anterior, existen ciertas situaciones en las que dicho tratamiento estará legitimado, siendo un claro ejemplo de ello la asistencia sanitaria[598]. A su vez, una forma tradicional de permitir dicho

[596] Artículo 89.1 del RGPD

[597] MÉSZÁROS, J. y HO, C. H. "Big data and scientific research: the secondary use of personal data under the research exemption in the GDPR". *Hungarian Journal of Legal Studies*, Vol. 59, Núm. 4, 2018, p. 416

[598] Los centros y los profesionales sanitarios de la red pública de salud no necesitan el consentimiento de los pacientes para tratar sus datos y así prestarles asistencia sanitaria. En el caso de los centros privados, es necesario realizar un contrato, el cual permitiría el tratamiento de los datos de los pacientes. El acceso

tratamiento ha sido la solicitud del consentimiento del interesado. En base al artículo 9.2.a) del RGPD, se podrá realizar el tratamiento de estos datos cuando el interesado haya otorgado su consentimiento explícito para el tratamiento de sus datos personales con uno o más fines especificados.

La exigencia de que el consentimiento sea específico, interpretada de una forma aislada y restrictiva, implicaría que el consentimiento y la información previa deberían ser prestados de manera particular para cada investigación, estudio o proyecto concreto. Esta posible interpretación alarmó a los investigadores, dado que lo concibieron como un ataque y una rémora para el desarrollo de la investigación científica y biomédica, debido a que, con frecuencia, no es posible determinar totalmente la finalidad del tratamiento de los datos personales con dichos fines en el momento de su recogida[599].

Sin embargo, el considerando 33 del RGPD señala que cuando no sea posible determinar totalmente la finalidad del tratamiento de los datos personales con fines de investigación científica en el momento de su recogida, los interesados podrán dar su consentimiento para determinados ámbitos de investigación científica que respeten las normas éticas reconocidas para ello, y añade que los interesados deben tener la oportunidad de dar su consentimiento solamente para determinadas áreas de investigación, o partes de proyectos de investigación, en la medida que lo permita la finalidad perseguida. En este considerando subyace la posibilidad de instrumentar un consentimiento "amplio" que acoja áreas de investigación[600]. Esto es, el RGPD permite otorgar un "consentimientos amplio" o "*broad consent*" en el ámbito de la investigación científica.

---

a una historia clínica para fines asistenciales corresponde, únicamente, a los profesionales que atienden al paciente, ya sea individualmente o como parte de un equipo de profesionales. Así, si una persona acude al médico o al centro sanitario para una consulta médica, el médico no tendrá que solicitarle el consentimiento para registrar la visita en una base de datos que contiene campos como su nombre y apellidos y la descripción de los síntomas. El tratamiento de estos datos relativos a la salud está permitido puesto que es necesario para atender a la persona, y se realiza bajo la responsabilidad de un médico que está sujeto a la obligación de secreto profesional. En el caso de que el médico le realice la receta médica en soporte papel o electrónico, tampoco le solicitará el consentimiento, puesto que en base al artículo 19.2 del Real Decreto 1718/2010, de 17 de diciembre, de receta médica, dicha actuación tiene por finalidad facilitar la asistencia médica y farmacéutica al paciente. Por tanto, en la relación ordinaria médico-paciente, el consentimiento para recibir la asistencia conlleva el consentimiento para el tratamiento de los datos de salud. La garantía o contrapeso de esta excepción es el deber de secreto y confidencialidad que radica en el profesional sanitario. Véase al respecto: APDCAT. Guia de protecció de dades per a pacients i usuaris dels serveis de salud, junio de 2020, p. 32; y BELTRÁN AGUIRRE, J. L., "La protección de los datos personales relacionados con la salud", *Ponencia presentada en el Defensor del Pueblo de Navarra*, 27 de junio de 2012, p. 62, disponible en: https://www.navarra.es/NR/rdonlyres/517A4434-9C3B-442E-8651-61A7AE0490AD/226320/pdps.pdf

[599] Hasta ahora, en el ámbito de la investigación clínica o biomédica siempre ha existido una relación médico-paciente y en un fin específico bien establecido. No obstante, en el caso de los proyectos de investigación que utilizan recursos de macrodatos en salud, a menudo es imposible delimitar los propósitos de la investigación que pretenden apoyar. Véase al respecto: VILLALOBOS-QUESADA, M., "Participative consent: Beyond broad and dynamic consent for health big data resources", *Revista de derecho y genoma humano*, Núm. Extra 1, 2019, p. 496

[600] BELTRÁN AGUIRRE, J.L. "Reglamento General de Protección de Datos: Novedades. Adaptación de la normativa española: el proyecto de LOPD", *Derecho y salud*, Vol.28, Núm. 1, 2018, p. 79

Este consentimiento amplio otorga a los investigadores la posibilidad de realizar un tratamiento de datos en un marco amplio de fines de investigación. Aunque el consentimiento amplio no ha de ser comprendido como un consentimiento general o abierto (también conocido como "*blanket consent*" o "*open consent*")[601], concede mayores oportunidades a los investigadores[602]. Esto demuestra que el RGPD permite una especificidad menos estricta en este ámbito. Si los Estados Miembros interpretan de una forma amplia y permisiva el Considerando 33 del RGPD, cabe el riesgo de que el requisito de que el consentimiento sea específico quede sin efecto en el ámbito de la investigación científica[603].

Cabe cuestionarse si un consentimiento tan amplio e inespecífico puede realmente ser considerado como un consentimiento válido. La falta de especificidad, y como consecuencia, falta de información, hacen peligrar la misma esencia del derecho a la protección de datos, dado que se impide que el interesado pueda tener una capacidad de control sobre sus datos personales. Por ello, la aplicación de este enfoque flexible requiere mayores garantías[604]. Cuando los fines de una determinada investigación no puedan especificarse en su totalidad, el responsable del tratamiento debe buscar otras maneras para proteger la esencia de los requisitos del consentimiento del interesado. Por ejemplo, puede solicitar a los interesados un consentimiento más general y otorgado para fases concretas de un proyecto de investigación que ya se conozcan desde el inicio. Posteriormente, a medida que la investigación avance, puede requerir el consentimiento para los siguientes pasos del proyecto, dicho consentimiento debe mantener su conformidad con las normas éticas aplicables a la investigación científica[605].

La transparencia se erige en una de las claves para hacer frente a la falta de concreción del fin. Los responsables del tratamiento podrán compensar esta falta concreción facilitando información periódica sobre el desarrollo del fin a medida que avanza el proyecto de investigación de manera que, con el transcurso del tiempo, el consentimiento se convierta en lo más específico posible. En consecuencia, el interesado o participante del proyecto, tendrá una noción básica del mismo, la cual irá especificándose a medida que se desarrolle la investigación, lo que le permitirá valorar, entre otras cuestiones, si desea retirar su consentimiento o no. Asimismo, contar con un plan integral de investigación al que los interesados puedan recurrir, podría contribuir a compensar la falta de concreción del fin. Este plan de investigación debería especificar

[601] RUMBOLD, J. M. M., y PIERSCIONEK, B., "The effect of the general data protection regulation on medical research", *Journal of medical Internet research*, Vol. 19, Núm. 2, 2017, p.2

[602] A diferencia del consentimiento general, el consentimiento amplio permite limitaciones específicas sobre el tratamiento futuro de los datos. En este sentido: WENDLER, D., "Broad versus Blanket Consent for Research with Human Biological Samples", Hasting center report, Vol. 43, Núm. 5, 2013

[603] MÉSZÁROS, J., "The Conflict Between Privacy and Scientific Research in the GDPR", IEEE, 2018, pp. 2-3, disponible en: 10.23919/PNC.2018.8579471

[604] En contra de esta interpretación y limitación del uso del consentimiento amplio para la investigación, se ha afirmado que, con la misma, se ha reducido significativamente que el consentimiento llegase a ser una base realista para el procesamiento datos personales. Véase al respecto: PELOQUIN, D.; DIMAIO, M.; BIERE, B. y BARNES, M., "Disruptive and avoidable: GDPR challenges to secondary research uses of data", *European Journal of Human Genetics*, Vol. 28, Núm. 6, 2020, p. 700

[605] CEPD. Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, *cit.*, p. 30

las cuestiones de la investigación y los métodos de trabajo previstos de la manera más clara posible[606]. Como principio general, el consentimiento debe ser privilegiado hasta cierto punto en la investigación en salud, puesto que, en caso contrario, se estarían anteponiendo los intereses de los investigadores sanitarios[607].

Es necesario que el Comité Europeo de Protección de Datos emita directrices que ayude a los Estados Miembros respetar el derecho a la protección del interesado al tiempo en que se fomente la investigación. Para ello, se requiere una mayor delimitación de los conceptos como "consentimiento amplio" entre otros. A su vez, a modo de crítica se puede alegar que introducir la posibilidad de otorgar un consentimiento amplio en un ámbito tan importante como la investigación científica en un considerando es reflejo de una técnica legislativa inadecuada, y que no detallar las medidas que deberá adoptar el responsable del tratamiento en dichas situaciones pone en peligro el derecho a la protección de datos personales de los interesados. Sin perjuicio de lo anterior, el consentimiento del interesado sigue siendo una herramienta adecuada para legitimar el tratamiento de los datos relativos a la salud con fines de investigación sanitaria, pero son necesarias unas pautas a nivel europeo para que el derecho a la protección de datos personales de los interesados sea respetado en todo momento.

El requisito de que el consentimiento sea libre cobra especial importancia en el caso de las personas mayores que decidan participar en un proyecto de investigación sanitario. Los responsables del tratamiento deben prestar especial atención a la condición de que este haya sido dado libremente. El consentimiento no debe constituir una base jurídica válida para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento[608].

3.1.2. Tratamiento necesario por razones de un interés público esencial e interés público en el ámbito de la salud pública:

El RGPD recoge situaciones en las que se podrá realizar el tratamiento de dichas categorías especiales de datos sin el consentimiento del interesado con fines de investigación en salud. No en vano, el RGPD reconoce que la salud constituye un bien individual intrínseco a cada individuo que hay que proteger de manera personal, pero incorpora también un matiz colectivo, cuya protección y desarrollo corresponde a los poderes públicos. Esa consideración social adquiere especial relevancia en el ejercicio

[606] Ibid., p. 33
[607] DOVE, E. S., y CHEN, J., "Should consent for data processing be privileged in health research? A comparative legal analysis", *cit.*, p. 129
[608] El Reglamento (UE) 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE (DOUE núm. 57, de 27 de mayo de 2014), aborda expresamente estos riesgos y exige que el investigador tenga en cuenta todas las circunstancias pertinentes, en particular, si el posible sujeto del ensayo pertenece a un grupo desfavorecido desde el punto de vista económico o social, o si se encuentra en una situación de dependencia institucional o jerárquica que podría influir de manera inapropiada en la decisión sobre su participación. Véase al respecto: CEPD. Dictamen 3/2019 sobre las preguntas y respuestas acerca de la relación entre el Reglamento sobre ensayos clínicos (REC) y el Reglamento general de protección de datos (RGPD) artículo 70, apartado 1, letra b), *cit.*, pp.6-7

del tratamiento de datos relativos a la salud, dado que, en virtud de la misma, los datos de una persona física pueden servir para otras finalidades más allá de la asistencia sanitaria individual[609].

En concreto, en base al artículo 9.2.g) del RGPD, los datos relativos a la salud[610] se podrán tratar sin solicitar el consentimiento del interesado si el tratamiento de datos es necesario por razones de un interés público esencial. Asimismo, según el artículo 9.2.i) del RGPD, se podrá realizar el citado tratamiento si este se efectúa por razones de interés público en el ámbito de la salud pública[611], como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios o la inspección de reclamaciones de los ciudadanos[612]. Es decir, el RGPD diferencia "el interés público esencial" y "el interés público en el ámbito en el ámbito de la salud pública", aunque esta diferenciación pueda llevar a confusión por no saber cuándo se ha de basar un tratamiento en el artículo 9.2.g) del RGPD y cuándo en el artículo 9.2.i) del RGPD.

El RGPD no concreta o define el sentido y alcance de las expresiones "interés público esencial"[613] e "interés público en el ámbito de la salud pública", delegando dicha labor a los Estados Miembros. No obstante, aunque el artículo 9.2.i) del RGPD no defina el término "interés público en el ámbito de la salud pública", pone como ejemplo, entre otros, la protección frente a amenazas transfronterizas graves para la salud. En este sentido, la Decisión 1082/2013/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud[614], define amenaza transfronteriza grave para la salud como una amenaza para la vida u otro grave peligro para la salud de origen biológico, químico, ambiental o desconocido que se propaga o implica un riesgo significativo de propagarse a través de las fronteras

[609] SERRANO PÉREZ, M. M., "El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del Reglamento General de Protección de Datos y de la Ley de Protección de Datos Personales y garantía de los derechos", *Estudios de Deusto*, Vol. 68, Núm. 2, 2020, p. 269

[610] El Considerando 52 del RGPD admite el tratamiento de categorías especiales de datos personales en base al interés público cuando exista una alerta sanitaria o para la prevención o control de enfermedades transmisibles y otras amenazas graves para la salud.

[611] A su vez, el Considerando 54 del RGPD recoge que el tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública.

[612] AEPD., Guía para pacientes y usuarios de la sanidad, noviembre 2019, p. 6, disponible en: https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf

[613] La AEPD en su informe jurídico núm. 2020/0086 de 22 de febrero de 2020 indicó que el tratamiento de datos de salud derivado de las pruebas médicas de aptitud psicofísica del cuerpo de policía, encuentra su base en el interés público esencial, dado que además de tener el compromiso de portar armas, realizan funciones de muy diversa índole que sirven a la sociedad y al interés general, por lo que es razonable sostener que existe un interés público esencial, en que éstos tengan una determinada aptitud psicofísica. Es decir, existe un interés público esencial en la existencia en la policía local de un personal cuyas condiciones psicofísicas estén acordes con la alta responsabilidad de las funciones que les atribuye el ordenamiento jurídico y en especial, el mantenimiento de la seguridad y del orden público que la legislación les impone, resultando así proporcional dicho tratamiento de datos con la finalidad pretendida y el interés al que sirve en última instancia.

[614] DOUE núm. 293, de 5 de noviembre de 2013

nacionales de los Estados miembros y que puede requerir coordinación a nivel de la Unión para garantizar un nivel elevado de protección de la salud humana[615].

Ambas bases exigen que se adopten medidas adecuadas y específicas para proteger los intereses y derechos fundamentales de los interesados, recogiéndose, en particular, el secreto profesional en el artículo 9.2.i) del RGPD. Por consiguiente, el responsable del tratamiento deberá adoptar medidas adecuadas y específicas para realizar el tratamiento de los datos relativos a la salud con el fin de salvaguardar el interés público.

Con el término "necesario" introducido en el artículo 9.2.g) del RGPD, el legislador europeo exige que el tratamiento de datos relativos a la salud se realice de una forma proporcionada para lograr el fin perseguido. Dicho tratamiento no será legítimo si existe otra fórmula menos intrusiva de lograr el objetivo[616]. En cuanto al concepto de "salud pública", este se recoge en el citado Considerando 54, el cual realiza una remisión a la definición del Reglamento (CE) 1338/2008, del Parlamento Europeo y del Consejo de 16 de diciembre de 2008[617]. Así, se entiende por salud pública todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines[618].

En concreto, debe existir una amenaza para la vida u otro grave peligro para la salud. Por ende, ha de entenderse que un interés público en el ámbito de la salud pública, a efectos de excepcionar el consentimiento del interesado, solo acoge como norma general las actuaciones y los estudios epidemiológicos y de salud pública cuya finalidad directa sea la prevención de un riesgo grave para la salud de la población como las enfermedades transmisibles, control de epidemias y de su propagación, amenazas transfronterizas graves y situaciones de urgencia humanitaria por catástrofes naturales o de origen humano. Su rápida detección exige un acceso a información multidisciplinaria y una correcta evaluación del riesgo o peligro, y la investigación en salud pública es fundamental para una adecuada respuesta ante amenazas sanitarias[619].

Los legisladores deben tener en cuenta los riesgos que puedan crearse para el individuo frente a los beneficios públicos que se podrán lograr. Una de las "pruebas de proporción o equilibrio" en el contexto de la investigación es el denominado "*duty of easy rescue*"

[615] BELTRÁN AGUIRRE, J. L.; GARCÍA LÓPEZ, F. J. Y NAVARRO SÁNCHEZ, C., "Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD", *sespas*, noviembre de 2017, p. 9, disponible en: https://sespas.es/wp-content/uploads/2018/02/SESPAS_informe_proteccion_datos_2017.pdf
[616] ICO. Guide to the General Data Protection Regulation (GDPR), 2 de agosto de 2018, p. 76
[617] DOUE núm. 354, de 31 de diciembre de 2008
[618] Considerando 54 del RGPD
[619] Ibid., p. 9

o "deber de rescate fácil", el cual puede definirse como la posibilidad de beneficiar a la sociedad sin riesgo o con un riesgo mínimo para el individuo[620]. Así, la investigación podrá llevarse a cabo sin el consentimiento del interesado cuando esta aporte un beneficio público significante y no cree riesgos al individuo o, estos últimos, sean mínimos. No obstante, este equilibrio no ha sido desarrollado en un criterio general aplicable a nivel europeo, con todos los riesgos que conlleva la falta de armonización en una cuestión como la presente[621].

El concepto del interés público no acoge aquellos estudios que, aunque pueden llegar a conclusiones que a la larga mejorarán la salud de la población por el conocimiento adquirido mediante los mismos, su realización no sea urgente en base a una necesidad social o general. Este tipo de investigaciones, entran en el régimen diseñado para la "investigación científica" del artículo 9.2.j) del RGPD. La actividad científica al que se refiere este último artículo del RGPD es una actividad de interés general, pero no reúne las notas de imperiosidad, gravedad e inminencia, que identifican al concepto del "interés público" de los artículos 9.2.g) y 9.2.i) del RGPD[622].

Ha de tenerse en cuenta qué tipo de investigaciones pueden basarse en el apartado g) e i) del artículo 9.2 del RGPD[623]. Según indica el Comité Europeo de Protección de Datos, el tratamiento de los datos relativos a la salud en el contexto de los ensayos clínicos puede considerarse necesario para el cumplimiento de una misión realizada en interés público cuando el desarrollo de los ensayos clínicos forme parte directamente del mandato, las misiones o las tareas conferidos a un organismo público o privado por el Derecho nacional[624].

3.1.3. Tratamiento necesario con fines de investigación científica:

El RGPD recoge en su artículo 9.2.j) que los datos relativos a la salud podrán ser objeto de tratamiento cuando sea necesario con fines de investigación científica[625]. Esta base

[620] PORSDAM MANN, S.; SAVULESCU, J. y SAHAKIAN, B. J., "Facilitating the ethical use of health data for the benefit of society: Electronic health records, consent and the duty of easy rescue", *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences*, Núm. 374, 2016, p. 2

[621] HANSEN, J.; WILSON, P.; VERHOEVEN, E.; KRONEMAN, M.; KIRWAN, M.; VERHEIJ, R. y VAN VEEN, E. B., *Assessment of the EU Member States' rules on health data in the light of GDPR*, Oficina de publicación de la UE, Luxemburgo, 2021, p.59

[622] BELTRÁN AGUIRRE, J. L.; GARCÍA LÓPEZ, F. J. Y NAVARRO SÁNCHEZ, C., "Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD", cit., p. 10

[623] Cuando los profesionales detecten casos relacionados con enfermedades de declaración obligatoria o brotes epidémicos, están obligados a comunicar dichas situaciones a las autoridades sanitarias. En base al artículo 2 de la orden SND/404/2020, de 11 de mayo, de medidas de vigilancia epidemiológica de la infección por SARS-CoV-2, el COVID-19, enfermedad producida por la infección por el virus SARS-CoV-2, es una enfermedad de declaración obligatoria urgente.

[624] EDPB. Dictamen 3/2019 sobre las preguntas y respuestas acerca de la relación entre el Reglamento sobre ensayos clínicos y el Reglamento general de protección de datos (RGPD), 23 de enero de 2019, p. 8

[625] En el considerando 159 del RGPD se incluye a la investigación financiada por el sector privado dentro del concepto del tratamiento de datos personales con fines de investigación científica que tiene cabida en el artículo 9.2.j) del RGPD.

legitimadora es fruto de la importancia que otorga el legislador europeo a dicha actividad, y es que, el análisis de los datos relativos a la salud permite a los investigadores obtener nuevos conocimientos de gran valor sobre condiciones o enfermedades médicas extendidas. La normativa destaca que la combinación de la información procedente de diversos registros facilita la investigación científica de enfermedades cardiovasculares, el cáncer o la depresión, tan comunes en nuestra sociedad, pero, como se ha dicho en reiteradas ocasiones, esta tarea no se puede llevar a cabo sin las condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros[626].

Tal y como sea expuesto en el capítulo precedente, como norma general, los datos deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines de conformidad con el artículo 5.1.b) del RGPD. En esta línea, el RGPD introduce en su artículo 6.4 del RGPD un test de compatibilidad[627]. Sin embargo, en el caso de la investigación no es necesario realizar la prueba de compatibilidad dado que existe una presunción de compatibilidad[628].

A su vez, el artículo 5.1.e) del RGPD permite que los datos personales sean conservados más tiempo del necesario para cumplir el fin para el que fueron recabados siempre que se traten, entre otros, con fines de investigación científica. Por todo ello, el legislador europeo sitúa la actividad de investigación en una posición privilegiada. Aunque esta posibilidad de realizar un tratamiento posterior en base a la presunción de compatibilidad es beneficiosa para la investigación científica, también plantea problemas desde la perspectiva del derecho a la protección de datos personales. La misma CEPD ha declarado que debido a la naturaleza transversal y compleja del presente tema, se requieren las directrices que el CEPD tiene previsto publicar sobre el tratamiento de datos relativos a la salud con fines de investigación científica[629].

El artículo 9.2.j) del RGPD exige que la base del Derecho de la Unión o de los Estados miembros que establece el tratamiento de datos sensibles con fines de investigación científica esté sujeto a las garantías adecuadas para salvaguardar los derechos y libertades de los interesados. Así, debido a la naturaleza sensible de los datos relativos a la salud y los riesgos que se plantean cuando se reutilizan con fines de investigación

[626] Considerando 157 del RGPD

[627] Esta prueba es una herramienta novedosa que ayuda a decidir si el nuevo propósito es compatible con el original. Para ello, se tendrá en cuenta: cualquier relación entre los fines para los cuales se recogieron los datos personales y los fines del tratamiento ulterior previsto; el contexto en que se hayan recogido los datos personales; el grado de sensibilidad de los datos personales; las posibles consecuencias que pueda acarrear el tratamiento ulterior a los interesados, y la existencia de garantías adecuadas. Véase al respecto: MÉSZÁROS, J. y HO, C. H. "Big data and scientific research: the secondary use of personal data under the research exemption in the GDPR, *cit.*, pp.405-406

[628] COMISIÓN EUROPEA., "¿Podemos utilizar los datos para otro fin?", *ec.europa.eu*, disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_es *[Última consulta: 28 de julio de 2021]*

[629] CEPD. Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19, *cit.*, p. 10

científica, tienen que adoptarse medidas rigurosas que garanticen un nivel de seguridad adecuado, tal como exige el artículo 32.1 del RGPD[630]. Todas estas medidas constituyen elementos de refuerzo introducidas para equilibrar la falta de consentimiento y consiguiente pérdida de control de los datos del interesado[631]. De conformidad con el artículo 89.1 del RGPD, dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular el respecto del principio de minimización de los datos personales[632]. A su vez, en la línea del Considerando 156 del RGPD, el mismo artículo destaca entre las medidas la seudonimización, siempre que de esa forma puedan alcanzarse los fines de la investigación. Por tanto, como norma general deberá aplicarse la medida de la seudonimización para tratar los datos relativos a la salud con fines de investigación. Sin embargo, la normativa recoge el tratamiento de los datos personales que permitan la identificación del sujeto siempre que, en caso contrario, no puedan lograrse los fines de la investigación. Esta puerta abierta que deja el legislador europeo obliga a los Estados Miembros a realizar un ejercicio de interpretación y decidir cuando existe realmente esa imposibilidad.

Tal y como se ha indicado en el capítulo tercero, en base al artículo 4.5 del RGPD, la seudonimización es el tratamiento que se da a los datos personales para que estos no puedan atribuirse al interesado sin emplear información adicional. Se trata de cambiar la denominación de los datos por seudónimos, de manera que se reduzca la posibilidad de identificar directamente a los interesados a través de estos datos, si no se cuenta con la información adicional que permita la identificación. Por lo tanto, seudonimizar los datos es realizar el tratamiento de datos personales sin la posibilidad de poder identificar a los interesados, pero sin llegar a eliminar el vínculo entre los datos personales y los titulares, como cambiar el nombre y apellidos del interesado por una clave numérica. Solo quien posee la información adicional que establece el vínculo entre los datos personales y el interesado, puede llegar a identificar a la persona[633]. Sin embargo, ha de tenerse en cuenta que la seudonimización no es un método de anonimización[634]. Esta técnica reduce la vinculabilidad de un conjunto de datos con la identidad del interesado pero sigue existiendo una alta probabilidad de identificar a la persona física de manera

---

[630] Ibid., p. 10

[631] SERRANO PÉREZ, M. M., "El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del Reglamento General de Protección de Datos y de la Ley de Protección de Datos Personales y garantía de los derechos", *cit.*, pp. 271-272

[632] STJUE (Sala Quinta), de 24 de febrero de 2022, SS SIA contra Valsts ieņēmumu dienests, C-175/20, ECLI:EU:C:2022:124

[633] AYUDA LEY DE PROTECCIÓN DE DATOS., "La seudonimización de los datos y su importancia en el nuevo RGPD", *ayudaleydeprotecciónd*atos, disponible en: https://ayudaleyprotecciondatos.es/2020/11/18/seudonimizacion-de-datos/ *[Última consulta: 28 de julio de 2021]*

[634] En este sentido, se ha recomendado abandona el concepto de anonimización para no generar falsas expectativas ni seguridades que dañan la confianza depositada por la sociedad en los procesos de creación y transferencia de conocimiento. En la era de la reidentificación es preciso establecerla seudonimizacion por defecto, y exigir que los responsables de los tratamientos demuestren desde el diseño de los proyectos en los que se usen tecnologías emergentes que no es posible la atribución de personaldiad a los conjuntos de datos que se utilizan para el desarrollo de algoritmos. Véase al respecto: DE LECUONA, I. "Aspectos éticos, legales y sociales del uso de la inteligencia artificial y el Big Data en salud en un contexto de pandemia", *cit.*, p. 164

indirecta, cobrando especial importancia en el caso de la investigación científica. En otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimos[635].

Debido a la naturaleza sensible de los datos relativos a la salud y los riesgos que plantea su reutilización con fines de investigación científica, se han de adoptar medidas rigurosas que garanticen un nivel de seguridad adecuado, aunque la normativa simplemente mencione la seudonimización como ejemplo de medidas técnicas y organizativas a adoptar. El RGPD no realiza ninguna lista de las medidas que han de ser comprendidas como apropiadas para garantizar un nivel de seguridad adecuado, dejando nuevamente esta labor en manos de los Estados miembros, lo cual es criticable.

3.2. El tratamiento de los datos relativos a la salud con fines de investigación científica en la pandemia:

En el caso de la crisis sanitaria provocada por el COVID-19, el consentimiento del interesado ha tenido un papel doble, siendo necesaria su solicitud tanto para el desarrollo de soluciones tecnológicas[636] como para la realización de investigaciones científicas con datos personales de salud de los interesados.

Respecto al primer caso, la tecnología se ha convertido en un arma estratégica para ganar la guerra al COVID-19. A la necesidad de test, mascarillas o respiradores, se le añade la necesidad de datos, de información, de tecnología, de infraestructura adecuada, pero también, como se ha comprobado, de respetar una serie de pautas éticas, de transparencia informativa y de cumplimiento normativo[637].

Las investigaciones científicas destinadas a luchar contra la pandemia han podido ampararse en el consentimiento del interesado[638]. Para que una persona haya podido

---

[635] GT29. Dictamen 05/2014 sobre técnicas de anonimización, 0829/14/ES (WP216), 10 de abril de 2014, p. 22

[636] Las webs y plataformas han sido útiles para gestionar las relaciones, contactos y movilidad de los contagiados o para controlar el cumplimiento de confinamientos generales y particulares. De igual modo, las aplicaciones informáticas han posibilitado el auto diagnóstico a través de la introducción de datos, implementando evaluaciones para saber si procedía hacer el test, entre muchos otros servicios. Estas aplicaciones voluntarias que se han utilizado para, entre otras cuestiones, controlar la propagación de la enfermedad (no con fines de investigación), se han basado en el consentimiento del interesado (artículo 9.2.a) del RGPD). El consentimiento no sirve como base legitimadora para el tratamiento de los datos personales si la instalación de la aplicación, su uso y transmisión de datos es condición para la prestación de salud, puesto que no debe haber ninguna consecuencia negativa para el usuario. En relación con lo antedicho, el tratamiento que han realizado las mismas no ha tenido como fin la investigación. Sin embargo, aunque las principales finalidades de las aplicaciones informáticas derivadas del COVID-19 son las expuestas, las mismas pueden ser una fuente de Big data muy variada de la que extraer información y conocimiento para la investigación en salud, por ello, las aplicaciones han de ser controladas para comprobar si están realizando un uso secundario de estos datos.

[637] MARZO PORTERA, A., "El interés público de los datos personales en tiempos del COVID-19", *hayderecho*, 10 de abril de 2020, disponible en: https://hayderecho.expansion.com/2020/04/10/el-interes-publico-de-los-datos-personales-en-tiempos-del-covid-19/ *[Última consulta: 29 de julio de 2021]*

[638] RODRÍGUEZ AYUSO, J.F., "Estado de alarma y protección de la privacidad en tiempos de pandemia: licitud del tratamiento de categorías especiales de datos", *Revista De Derecho Político*, Núm. 110, 2021, p. 309

participar, por ejemplo, en un ensayo clínico de una vacuna contra el COVID-19, ha tenido que otorgar dos consentimientos: el consentimiento informado y el consentimiento del interesado. Tal y como se ha expuesto en el capítulo precedente, mediante el consentimiento informado, el sujeto acepta participar en el ensayo clínico y ser inyectado con la vacuna en cuestión. Por otra parte, mediante el consentimiento del interesado, acepta el tratamiento de sus datos, acción necesaria que el tratamiento de la información sensible generada durante el ensayo pueda procesarse por parte de los investigadores [639]. Los datos de los ensayos clínicos son analizados y cuando se decida, en base a los mismos, que la vacuna es segura, se solicita la autorización de la comercialización[640].

Aunque no siempre sea fácil decidir si el tratamiento de datos relativos a la salud supone un nivel de interés público[641] suficiente, en el caso de la crisis provocada por el COVID-19, se ha podido realizar el tratamiento de los datos relativos a la salud con fines de investigación por motivos importantes de interés público[642]. En este punto, puede producirse una situación de abuso por parte de los organismos públicos, dado que debajo del paraguas del interés público puede justificarse casi cualquier tratamiento de los datos relativos a la salud para la investigación en salud. Es preciso subrayar que ni siquiera ante una situación como la vivida se puede permitir cualquier tratamiento de datos con fines de investigación en salud en base al interés público, y que los tratamientos de datos relativos a la salud con fines de investigación que se realizan en situaciones de emergencia sanitaria en base al interés público no pueden convertirse en prácticas habituales. Aunque el tratamiento de los datos relativos a la salud con fines de investigación sea necesario y su valor incuestionable, no por ello ha de admitirse cualquier tipo de investigación con datos relativos a la salud, la sociedad debe confiar en las autoridades públicas[643].

Con el objetivo de analizar el tratamiento de los datos relativos a la salud con fines de investigación que se ha realizado en el ámbito de la pandemia, en este capítulo se estudiará el caso particular de España, Italia e Irlanda, estudiando las bases legales que han sido utilizadas en cada caso.

---

[639] BAIXAULI FERNÁNDEZ, V. J., y ABELLAN-GARCÍA SÁNCHEZ, F., "El consentimiento y el tratamiento de los datos relativos a la salud del paciente en la prestación y realización de estudios de investigación de servicios profesionales farmacéuticos asistenciales", *Farmacéuticos comunitarios*, Vol.11, Núm. 1, 2019, p. 27

[640] AEM., "COVID-19 vaccines", *ema.europa.eu*, disponible en: https://www.ema.europa.eu/en/human-regulatory/overview/public-health-threats/coronavirus-disease-covid-19/treatments-vaccines/covid-19-vaccines https://hayderecho.expansion.com/2020/04/10/el-interes-publico-de-los-datos-personales-en-tiempos-del-covid-19/ *[Última consulta: 29 de julio de 2021]*

[641] RUBÍ NAVARRETE, J., "La protección de datos personales en la pandemia de COVID-19", *Comunicaciones en propiedad industrial y derecho de la competencia*, Núm. 90, 2020, p. 7

[642] CEPD. Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19, *cit.*, p. 5

[643] MALGIERI, G., "Data Protection and Research: A vital challenge in the era of Covid-19 Pandemic", *Computer Law & Security Review*, Núm. 37, 2020, pp. 1-3

4. EL TRATAMIENTO DE LOS DATOS CON FINES DE INVESTIGACIÓN EN SALUD EN LA LOPDGDD:

Siguiendo lo dispuesto en el artículo 9.4 del RGPD, el legislador estatal ha desarrollado las bases legitimadoras para el tratamiento de los datos en la investigación en salud en el punto dos de la Disposición Adicional Decimoséptima (D.A.17ª) de la LOPDGDD. Compuesto de 8 letras, en el primero de ellos se identifica el consentimiento como base legitimadora para el tratamiento de los datos, y en las siguientes tres letras (b, c y d), se recogen las restantes bases legitimadoras. Así, la LOPDGDD recoge situaciones en las que el tratamiento de datos con fines de investigación en salud será legítima sin el consentimiento del interesado. En relación al artículo 89 del RGPD, en las letras f, g y h de la D.A.17ª de la LOPDGDD se exponen las medidas que se han de adoptar para proceder a realizar el tratamiento de datos en la investigación en salud con todas las garantías. Debido a las finalidades expresadas en los expositivos y la interpretación que realiza en su articulado conforme al RGPD, la LOPDGDD tiene vocación de facilitar la investigación[644].

4.1. Bases legales contempladas en la LOPDGDD:

4.1.1. El consentimiento del interesado o su representante legal:

Siguiendo la línea establecida por el artículo 9.2.a) del RGPD, en el apartado 2.a) de la Disposición Adicional Decimoséptima, se recoge que el interesado o su representante legal podrán otorgar el consentimiento para el uso de sus datos con fines de investigación en salud y en particular la biomédica. Seguidamente, se expone que tales finalidades podrán abarcar categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora. Por tanto, el consentimiento del interesado podrá extenderse o ampliarse a áreas generales vinculadas a una especialidad médica o investigadora. Así, puede afirmarse que el legislador español ha optado permitir el recurso al consentimiento amplio en la normativa[645].

En el ámbito de la investigación científica, el requisito de especificidad del consentimiento no se interpreta de un modo restrictivo en la LOPDGDD, pudiendo extenderse en el futuro ese consentimiento, sin que ello lo vicie, incluso a "finalidades" o áreas de investigación que ni siquiera hubieran podido determinarse en el momento en que se prestó el consentimiento. Esta amplificación o extensión del consentimiento hace

[644] MARTÍNEZ MARTÍNEZ, R. Y ÁLVAREZ RIGAUDIAS, C., "El uso de datos con fines de investigación biomédica (arts.9 y 89 RGPD. Art 9, Disposición Adicional decimoséptima, Disposición final novena y Disposición transitoria sexta LOPDGDD)", en LÓPEZ CALVO, J., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Wolters Kluwer, Madrid, 2019, p. 279

[645] MÉNDEZ GARCÍA, M. y ALFONSO FARNÓS, I., "La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018", *Revista de derecho y genoma humano*, Vol. 205, Núm. 231, 2019, p. 213

que no sea necesario recabar un nuevo consentimiento para que pueda realizarse el tratamiento de los datos personales[646].

Debido a la poca claridad del legislador a la hora de redactar la Disposición Adicional objeto del presente análisis, el contenido de la letra a) puede llegar a confundirse con el contenido de la c). La letra a) regula el supuesto de un consentimiento explícito ab initio para fines de investigación en salud que abarquen áreas generales vinculadas a especialidades médicas o investigadoras. Por su parte, tal y como se analizará más adelante, la previsión de la letra c) está destinada a permitir que un consentimiento explícito para una investigación concreta pueda a posteriori permitir la licitud de tratamientos con fines de investigación en salud relacionados con el área en la que se integró el estudio inicial para el cual se prestó el consentimiento[647].

Por ejemplo, mediante el apartado a) una persona puede otorgar su consentimiento para que sus datos sean utilizados para la investigación del cáncer de pulmón. Este consentimiento podrá ampliarse a áreas generales vinculadas a una especialidad médica o investigadora, como puede ser la oncológica. No obstante, en base a la letra c), el centro que obtuvo el consentimiento para un estudio concreto, podrá reutilizar los datos que se recolectaron para el estudio inicial en otro estudio posterior que se integre en la misma área de investigación. Por ende, aunque la redacción de las citadas letras pueda llevar a confusión, se trata de dos cuestiones distintas.

La utilización del consentimiento del interesado para categorías relacionadas con áreas generales vinculadas a una especialidad médica o investigadora deberá ser determinada por el responsable del tratamiento, tras una valoración de la vinculación entre finalidades realizada por el profesional investigador. Por tanto, el responsable del tratamiento tendrá en cuenta el criterio del experto para señalar si existe conexión material o funcional para poder determinar la validez del consentimiento del interesado. Por tanto, la novedad que aporta este apartado es la posibilidad de realizar investigaciones en salud a partir de un consentimiento "cuasi genérico" otorgado para investigar en relación con especialidades médicas o investigadoras generales[648].

Aunque el apartado 2.a) de la D.A. 17ª de la LOPDGDD utilice la expresión "*el interesado o, en su caso, su representante legal*", tras la entrada en vigor de la Ley 8/2021 que ha sido analizada en el capítulo 2 de este trabajo, se ha de reinterpretar la presente base legitimadora y comprender que, en adelante, la persona con discapacidad podrá otorgar su consentimiento con los apoyos que necesite para que sus datos relativos a la salud sean tratados con fines de investigación en salud. Cobra una especial relevancia la necesidad de adaptar la información sobre el tratamiento de los datos

[646] AEPD. Informe jurídico núm. 073667/2018, de 5 de marzo de 2018
[647] EMALDI CIRIÓN, A., "Protección de datos personales en el ámbito sanitario y de investigación biomédica: Una visión europea", *Actualidad Jurídica Iberoamericana*, Núm.14, 2021, p. 735
[648] SERRANO PÉREZ, M. M., "El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del Reglamento General de Protección de Datos y de la Ley de Protección de Datos Personales y garantía de los derechos", *cit.*, p. 277
[648] ICO., Guide to the General Data Protection Regulation (GDPR), 2 de Agosto de 2018, p. 76

personales y sobre la participación en la investigación a las distintas condiciones y capacidades de las personas con discapacidad[649]. Igualmente, el curador representativo podrá en base a la voluntad, intereses y preferencias[650] de la persona con discapacidad otorgar los relativos consentimientos por representación en las situaciones más extremas.

En caso de que el tratamiento de los datos relativos a la salud con fines de investigación en salud sea contrario a la voluntad del interesado, la única forma de realizar el tratamiento será justificarlo en otra base legal del apartado segundo de la D.A. 17ª de la LOPDGDD. Si no se puede aplicar la base legal del consentimiento del interesado, se deberá analizar si es de aplicación alguna de las bases restantes del apartado segundo de la D.A. 17ª de la LOPDGDD, lo cual permitiría realizar el tratamiento de los datos relativos a la salud con fines de investigación sin el consentimiento del interesado. Por ejemplo, si estuviésemos ante una situación de excepcional relevancia y gravedad para la salud pública, las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrían realizar dicho tratamiento aunque no existiera el consentimiento del interesado.

4.1.2. Situación de excepcional relevancia y gravedad para la salud pública:

En el apartado b) del punto 2 de la Disposición Adicional Decimoséptima se recoge que las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados en situaciones de excepcional relevancia y gravedad para la salud pública[651].

---

649 NICOLÁS JIMÉNEZ, P., y TERRIBAS I SALA, N., "Investigación con datos de carácter personal", en ROMEO CASABONA, C.M (dir.); NICOLÁS JIMÉNEZ, P., y ROMEO MALANDA, S. (coord.), *Manual de bioderecho (Adaptado para la docencia en ciencias de la salud y ciencias sociales y jurídicas)*, Dykinson, Madrid, 2022, p. 700

650 En este sentido, la recomendación nº R (97) 5, de 13 de febrero de 1997, del Comité de Ministros del Consejo de Europa a los Estados miembros sobre Protección de Datos Médicos recoge en su apartado 6.3 que, cuando se trate de procesar datos médicos de una persona legalmente incapacitada que es incapaz de una decisión libre, y cuando la ley nacional no le permita actuar en su propia representación, es preciso obtener el consentimiento de la persona legalmente habilitada para actuar en interés de éste, o de la autoridad o persona u órgano designados por la ley con este fin, pero que se deberán tener en cuenta sus deseos a menos que la ley nacional disponga otra cosa. Si el uso de otra base legal no tiene fundamento, no se podrá realizar el tratamiento de los datos relativos a la salud con fines de investigación en salud.

651 La AEPD analizó en su informe jurídico núm. 2018/0121 de 9 de enero de 2019 si existe una habilitación legal por parte de los organismos titulares de las bases de datos clínicos para la cesión de los mismos sin necesidad del consentimiento del interesado. La consulta fue planteada por el CNE, centro estatal perteneciente al Instituto de Salud Carlos III (SCIII), el cual desarrolla tareas en relación con la vigilancia de algunas enfermedades sujetas a un régimen de declaración obligatoria como el sida o la tuberculosis. Según alega el centro, para la identificación de factores de riesgo y para la vigilancia de las patologías, precisan acudir al cruce de datos clínicos y administrativos. Tal y como se analiza en el informe, el artículo 41 de la ley 33/2011, de 4 de octubre, General de Salud Pública, establece que las autoridades sanitarias con el fin de asegurar la mejor tutela de la salud de la población podrán requerir a los servicios y profesionales sanitarios informes, protocolos u otros documentos con fines de información sanitaria. Las Administraciones sanitarias no precisarán obtener el consentimiento de las personas afectadas para el tratamiento de datos personales, relacionados con la salud, así como su cesión a otras Administraciones públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población. A los efectos indicados, las personas públicas o privadas cederán a la autoridad sanitaria,

Es claro que, el legislador estatal se ha basado en las bases jurídicas de las letras g) e i) del artículo 9.2 del RGPD a la hora de redactar este apartado. A su vez, el legislador español limita expresamente la aplicación de esta base legitimadora a las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública, excluyendo a las empresas privadas[652].

Se habilita el tratamiento de datos sin consentimiento del interesado siempre que dicho tratamiento se lleve a cabo por parte de las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública, y únicamente si concurren circunstancias de excepcional relevancia y gravedad para la salud pública. En aquellos casos en los que no concurra la situación de excepcional relevancia y gravedad, no se permitirá el tratamiento de datos sin el consentimiento del interesado salvo que sea aplicable otra base legitimadora[653].

El Comité de Bioética de España en su informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de Covid-19, declaró que, en situaciones de excepcional relevancia y gravedad para la salud pública, contexto que concurre en el caso de la pandemia provocada por el COVID-19, las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública podrán llevar a cabo estudios científicos sin el consentimiento de los afectados e incluso manteniéndose los datos de identificación del sujeto fuente. Por tanto, cabría un uso secundario muy amplio, no sujeto ni al requisito del nuevo consentimiento, ni al de la anonimización, ni tampoco al de la seudonimización. Eso sí, se trataría de estudios que estuvieran enmarcados en el estricto ámbito de las autoridades públicas[654]. En suma, la letra b) de la Disposición Adicional Decimoséptima permite al responsable del tratamiento, realizar estudios científicos con datos relativos a la salud sin necesidad de contar con el consentimiento del interesado, siempre que la excepcionalidad, relevancia y gravedad de la situación para la salud pública así lo aconseje[655].

Con todo, el principio de minimización de datos no deja de operar en el contexto de la pandemia, de manera que los datos tratados habrán de limitarse exclusivamente a los

---

cuando así se las requiera, los datos de carácter personal que resulten imprescindibles para la toma de decisiones en salud pública. Las expresiones "estrictamente necesario" e "imprescindible" del citado artículo ponen de relieve la interpretación que ha de realizarse respecto del tratamiento de estos datos personales, dado que el legislador no ha previsto que todo tipo de datos personales relacionados con la salud pueda ser libremente y sin restricciones cedidos o transmitidos entre administraciones públicas, sino exclusivamente por razones imprescindibles. En consecuencia, la AEPD resolvió que no se requiere el consentimiento de las personas afectadas para la cesión por las Administraciones Públicas al CNE de datos personales relacionados con la salud por razones de salud pública o por razones epidemiológicas.

[652] EMALDI CIRIÓN, A., "Protección de datos personales en el ámbito sanitario y de investigación biomédica: Una visión europea", *cit.*, p. 736

[653] APDCAT. Dictamen en relació amb la consulta d'un centre sanitari sobre la necessitat del consentiment en el cas de la utilització de dades de salut seudonimitzades en investigació biomédica CNS 15/2019, de 14 de mayo de 2019, pp. 13-14

[654] CBE. Informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de Covid-19, 28 de abril de 2020, p. 16

[655] RODRÍGUEZ AYUSO, J.F., "Estado de alarma y protección de la privacidad en tiempos de pandemia: licitud del tratamiento de categorías especiales de datos", *cit.*, p. 315

necesarios para la finalidad pretendida, sin que pueda confundirse conveniencia con necesidad. La conservación de esos datos no se extenderá más allá de la duración y finalidad de la investigación[656].

La salvaguardia de intereses esenciales en el ámbito de la salud pública corresponde a las distintas autoridades sanitarias de las diferentes administraciones públicas, quienes podrán adoptar las medidas necesarias para salvaguardar dichos intereses esenciales públicos en situaciones de emergencia sanitaria de salud pública[657].

4.1.3. Reutilización de los datos personales:

Tal y como se adelantado anteriormente, en el apartado 2.c) de la citada Disposición Adicional se dispone que se considerará lícita y compatible[658] la reutilización de datos personales con fines de investigación en materia de salud y biomédica cuando, habiéndose obtenido el consentimiento para una finalidad concreta, se utilicen los datos para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial. No se solicitará de nuevo el consentimiento si los datos se utilizan para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial.

En otras palabras, la letra c) de la Disposición Adicional Decimoséptima prevé la posibilidad de reutilizar datos personales con fines de investigación sin necesidad de recabar nuevamente el consentimiento de los interesados, habilitando así el tratamiento de datos que inicialmente fueron recogidos para una finalidad determinada con el consentimiento del interesado. La presente habilitación para la reutilización de los datos encuentra su origen en el artículo 9.2.j) del RGPD, puesto que el mismo admite como finalidad compatible la investigación científica en los términos del artículo 89 del RGPD[659]. Se valida la reutilización de los datos recogidos previamente para una finalidad investigadora concreta y consentida por el interesado para investigaciones posteriores, siempre que puedan establecerse relaciones entre ambas. El legislador apuesta, de nuevo, por el consentimiento amplio para no obstaculizar la investigación, dado que, en la letra c) se prevé la posibilidad de autorizar el tratamiento de datos para

[656] CBE. Informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de Covid-19, *cit.*, p. 21

[657] AEPD. Informe jurídico núm. 2020/0017 de 12 de marzo de 2020

[658] La AEPD en su Informe núm. 0317/2009 de 16 de febrero de 2010 analizó si una Universidad Pública podía solicitar a otra Universidad Pública los datos de estudiantes con discapacidad matriculados en la misma para la realización de un estudio científico. Al tratarse de datos de minusvalía, se trataba de un tratamiento de datos de salud con fines científicos. La Agencia Española de Protección de Datos resolvió que los datos fueron recogidos y tratados para el adecuado cumplimiento de la relación jurídica existente entre la Universidad y quienes se matricularon en ella para recibir formación académica, y que por tanto, la finalidad de la recogida de dichos datos era incompatible con la finalidad del estudio científico. Por todo ello, no existía excepción al deber de solicitar el consentimiento.

[659] APDCAT. Dictamen en relació amb la consulta d'un centre sanitari sobre la necessitat del consentiment en el cas de la utilització de dades de salut seudonimitzades en investigació biomédica CNS 15/2019, *cit.*, pp. 7-8

investigaciones no previstas inicialmente, pero vinculadas con la investigación consentida[660].

La reutilización ha de ser entendida como un uso o un tratamiento secundario de los datos de salud para una finalidad compatible con la finalidad inicial para la que se recogieron los datos. A su vez, la Disposición Transitoria Sexta del LOPDGDD indica que se considerará lícita y compatible la reutilización con fines de investigación en salud y biomédica de datos personales recogidos con anterioridad a la entrada en vigor de la LOPDGDD sobre la base del consentimiento que habrían prestado los interesados para el estudio inicial.

De la lectura del citado apartado, se deduce que los datos reutilizados deben proceder de otros estudios, no pudiendo tratarse de datos recogidos con fines asistenciales, y es que, al hablar de "estudio inicial", queda patente que los datos personales fueron recogidos estrictamente con fines de investigación. El tratamiento de datos procedentes de las historias clínicas de los pacientes tendrá otra base legitimadora como la indicada en el apartado d) de la Disposición Adicional objeto de estudio[661].

Corresponderá al Comité de Ética de la Investigación (CEI) valorar si el área de investigación para la que se solicita autorización está realmente relacionada con el área en la que se integraba el estudio inicial. Este acto de valoración puede crear opiniones dispares dentro del CEI, por tanto, la Comisión Europea de Protección de Datos debería emanar unas directrices. Así, los CEI, sin los que no es posible avanzar en investigación, pues de ellos depende la aprobación de los proyectos, se convierten en actores fundamentales del sistema de investigación y también de la innovación aparejada en salud. Su dictamen previo y favorable es "*conditio sine qua non"* para que puedan desarrollarse los citados proyectos. Aunque inicialmente los CEI se crearon para evaluar ensayos clínicos con medicamentos y productos sanitarios, en los últimos tiempos evalúan también proyectos de investigación e innovación que utilicen tecnologías emergentes como la inteligencia artificial, el Big Data, y en los que se desarrollen de dispositivos y aplicaciones de salud[662]. Los CEI responden a una obligación legal, metodológica y ética a la hora de evaluar con carácter previo los distintos proyectos de investigación que se proponen[663].

En base al artículo 13.1 del RGPD, cuando el CEI entienda que el área de investigación está relacionada con el área en la que se integraba el estudio original, para cumplir con

[660] SERRANO PÉREZ, M. M., "El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del Reglamento General de Protección de Datos y de la Ley de Protección de Datos Personales y garantía de los derechos", *cit.*, p. 278

[661] MÉNDEZ GARCÍA, M. y ALFONSO FARNÓS, I., "La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018", *cit.*, pp. 217-218

[662] DE LECUONA, I. "Aspectos éticos, legales y sociales del uso de la inteligencia artificial y el Big Data en salud en un contexto de pandemia", *cit*., p. 159

[663] VALCÁRCEL TEIJEIRO, N. "Protección de datos de salud e investigación hospitalaria", en GÓMEZ PIQUERAS, C.; MARTÍNEZ MARTÍNEZ, R.; PÉREZ GÓMEZ, J.M.; ROMEO CASABONA, C.M.; SÁNCEZ CARP, J. y VALCÁRCEL TEIJEIRO, N. *Protección de datos e investigación médica*, Aranzadi, Pamplona, 2009, p. 103

la exigencia de garantías adecuadas del artículo 89.1 del RGPD, los responsables deberán publicar la información establecida por el mismo artículo del RGPD en un lugar fácilmente accesible de la página web corporativa del centro donde se realice la investigación o estudio clínico, y, en su caso, en la del promotor, y notificar la existencia de esta información por medios electrónicos a los afectados. Cuando estos carezcan de medios para acceder a dicha información, podrán solicitar su remisión en otro formato. En definitiva, la normativa permite un tratamiento posterior de los datos personales siempre que sea compatible con el inicial, y exige al responsable del tratamiento que cumpla con su obligación de informar al interesado.

El interesado tendrá la posibilidad de oponerse a la reutilización de sus datos personales para sucesivas finalidades de investigación. Por ello, en la información que ha de hacerse visible en la página web del centro o que se envía por correo ha de quedar especialmente clara la forma de ejercitar los derechos por parte de los interesados y dentro de ellos el derecho de oposición al tratamiento. La falta de información acerca del ejercicio de los derechos o la falta de claridad pueden ser interpretadas como una lesión en el núcleo fundamental del derecho a la protección de datos y por tanto una vulneración del derecho mismo[664].

Sin perjuicio de lo anterior, la Disposición Transitoria 6 de la LOPDGDD permite la reutilización de datos relativos a la salud provenientes de proyectos de investigación preexistentes recogidos antes de la entrada en vigor de la LOPDGDD siempre que los datos se utilicen para finalidades o áreas de investigación relacionadas con la especialidad médica o investigadora en la que se integrase científicamente el estudio inicial.

4.1.4. Datos personales seudonimizados:

En la línea de lo dispuesto en el artículo 9.2.j) del RGPD, el apartado d) de la Disposición Adicional Decimoséptima de la LOPDGDD recoge que se considera lícito el uso de datos personales seudonimizados con fines de investigación en salud y, en particular, biomédica, sin que sea necesario el consentimiento del interesado. La licitud para la utilización de datos seudonimizados con fines de investigación en salud sin el consentimiento del interesado pasa necesariamente por el cumplimiento de las medidas que establece el artículo 9.2.j) en conexión con el artículo 89.1 del RGPD. Así, incluso en el caso de que la finalidad de un tratamiento pueda considerarse propia de la investigación en el ámbito de la salud, el responsable del tratamiento deberá adoptar las medidas adecuadas para garantizar la protección de los datos personales[665]. A diferencia del apartado 2.b) de la Disposición Adicional objeto de estudio, las empresas privadas

[664] STJUE (Sala Segunda) de 20 de diciembre 2017, Peter Nowak v. Data Protection Commissioner, Asunto C-434/16, ECLI:EU:C:2017:994

[665] APDCAT. Dictamen en relació amb la consulta d'un centre sanitari sobre la necessitat del consentiment en el cas de la utilització de dades de salut seudonimitzades en investigació biomédica CNS 15/2019, *cit.*, p. 13

podrán acogerse a esta base legitimadora para realizar tratamientos de datos con fines de investigación en salud.

Como garantía de la seudonimización, se requiere una separación técnica y funcional entre el equipo investigador y quienes realicen la seudonimización y conserven la información que posibilite la reidentificación. Los investigadores podrán acceder a dichos datos cuando exista un compromiso expreso de confidencialidad y de no realizar ninguna actividad de reidentificación, y se adopten medidas de seguridad específicas para evitar la reidentificación y el acceso de terceros no autorizados. Sin embargo, podrá realizarse la reidentificación de los datos cuando se aprecie la existencia de un peligro real y concreto para la seguridad o salud de una persona o grupo de personas, una amenaza grave para sus derechos o sea necesaria para garantizar una adecuada asistencia sanitaria. Por tanto, en base a la D.A.17ª.2.d) de la LOPDGDD, si una persona consiente el tratamiento de sus datos relativos a la salud para la investigación de una determinada enfermedad, no se le requerirá de nuevo el consentimiento para realizar otra investigación que esté relacionada con la inicial. Para realizar esta nueva investigación, se seudonimizarán los datos relativos a la salud, y solo se podrá proceder a la reidentificación si su salud o derechos están en juego. En base al apartado g) de la Disposición Adicional Decimoséptima de la LOPDGDD, se requerirá un informe previo de un Comité de Ética de la Investigación o bien en su defecto, de un delegado de protección de datos o un experto con los conocimientos en la materia.

En nuestra opinión, cabe criticar la redacción del segundo parágrafo del apartado d), puesto que, mediante una interpretación estricta de la frase "con fines de investigación en salud pública y biomédica requerirá" se puede entender que las medidas aplicables a la seudonimización son solo aplicables a la investigación pública, no a la privada, que sin embargo, no está excluida de la posibilidad de llevar a cabo este tipo de proyectos. No obstante, dicha afirmación concedería un privilegio no justificado a los estudios privados, dado que, a diferencia de los estudios públicos, no tendrían que realizar la seudonimización para realizar la nueva investigación. Por tanto, se ha de comprender que esta obligación se aplica tanto a la investigación pública como a la privada.

4.2. Garantías aplicables al tratamiento de datos en la investigación sanitaria:

En base a los artículos 9.2.j) y 89 del RGPD, el tratamiento de datos en investigación sanitaria requiere la implementación de ciertas garantías. Debido a la poca claridad de la redacción de la Disposición Adicional Decimoséptima de la LOPDGDD, puede dar lugar a interpretaciones dispares.

En el apartado 2.f) de la Disposición Adicional Decimoséptima de la LOPDGDD se recogen las garantías que ha de reunir cualquier tratamiento de datos con fines de investigación en salud pública y, en particular, biomédica. Al igual que se ha alegado en el apartado anterior, al referirse a la "salud pública", puede llegar a interpretarse que dichas garantías han de ser adoptadas únicamente para las investigaciones realizadas por las autoridades sanitarias e instituciones públicas, no siendo aplicables a las

investigaciones privadas. En nuestra opinión, dicha afirmación otorgaría un privilegio especial a las investigaciones realizadas por el sector privado, y a su vez dejaría sumamente desprotegido al interesado cuyos datos serían objeto de tratamiento, se ha de comprender que en el referido apartado f) se recogen las garantías que han de aplicarse a cualquier tratamiento de datos con fines de investigación en salud, no distinguiendo entre la actividad pública y la privada.

Se deben cumplir cuatro acciones para realizar cualquier investigación en salud. Para empezar, se ha de realizar una evaluación de impacto que establezca los riesgos derivados del tratamiento de datos en los supuestos previstos en el artículo 35 del RGPD o en los establecidos por la autoridad de control. La citada evaluación de impacto es obligatoria en este campo, ya que se realiza un tratamiento de las categorías especiales de datos a que se refiere el artículo 9.1 del RGPD, y así lo indica expresamente la AEPD en el punto cuatro de su lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos[666].

En el apartado 7 del artículo 35 del RGPD se identifican los cuatro elementos que componen el contenido mínimo de una evaluación de impacto[667]. El primer elemento trata de una descripción sistemática de las operaciones de tratamientos previstas y de los fines del tratamiento, incluyendo, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento. Asimismo, se deberá realizar una evaluación de la necesidad y de la proporcionalidad de las operaciones del tratamiento con respecto a su finalidad. El tercer elemento se refiere a la evaluación de los riesgos que el tratamiento entraña para los derechos y libertades de los interesados. Por último, se deberán exponer las medidas previstas para hacer frente a los riesgos detectados, lo que incluye garantías, medida de seguridad y mecanismos que protejan los datos personales. A su vez, a estos cuatro elementos que identifica en RGPD, hay que sumarles los riesgos de reidentificación vinculados a la anonimización o seudonimización de los datos que expresamente suma la LOPDGDD. En este punto, cabe criticar que el legislador español introduzca la frase "los riesgos de reidentificación vinculados a la anonimización", puesto que, según la misma definición de la anonimización, este proceso hace imposible

[666] AEPD., "Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)", *aepd*, 4 de septiembre de 2019, disponible en: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

[667] La Oficina del Delegado de Protección de Datos de la Fundación TIC Salud Social en colaboración con un equipo multidisciplinar del Observatorio de Bioética y Derecho de la Universidad de Barcelona, presentaron el 9 de febrero de 2021 una metodología y una herramienta ágil para llevar a cabo una evaluación de impacto basada en el modelo de la Autoridad Catalana de Protección de Datos. Esta propuesta se ha adaptado a las necesidades específicas del ámbito de salud para evaluar los tratamientos de datos personales en procesos de investigación y de innovación. Los resultados son una metodología y una herramienta ágil, que permite una autoevaluación para detectar riesgos en el tratamiento de datos personales y su mitigación mediante un lenguaje sencillo; con definiciones y ejemplos para identificar los actores y describir los tratamientos, y que permite medir los riesgos para establecer un plan de acción. Véase al respecto: OBSERVATORIO DE BIOÉTICA Y DERECHO DE LA UNIVERSIDAD DE BARCELONA., "Presentada la metodología de evaluación de impacto relativa a la protección de datos en salud", *bioeticayderecho*, 9 de febrero de 2021, disponible en: http://www.bioeticayderecho.ub.edu/es/presentada-la-metodologia-de-evaluacion-del-impacto-relativa-la-proteccion-de-datos-en-salud *[Última consulta: 31 de julio de 2021]*

que se pueda volver a identificar a los interesados, quedando fuera de la aplicación del RGPD. Cuestión distinta es que, como bien se viene advirtiendo en el transcurso del presente trabajo, hoy en día la anonimización sea realmente irreversible o no. Así, parece que el mismo legislador admite dicha posibilidad, y exige que se expongan los riesgos en cada caso.

El segundo punto es relativo al cumplimiento de las normas de calidad. En este sentido, el CIOMS en colaboración con la OMS creó el documento de las "pautas éticas internacionales para la investigación relacionada con la salud con seres humanos", en el cual se indican las normas a seguir para cumplir con los estándares de calidad[668]. En tercer lugar, se han de adoptar medidas dirigidas a garantizar que los investigadores no tengan acceso a datos de identificación de los interesados. Por último, se deberá designar a un representante legal establecido en la UE, de acuerdo con el artículo 74 del citado Reglamento 536/2014, si el promotor del ensayo clínico no está establecido en la UE. Dicho representante podrá coincidir con el previsto en el art. 27.1 del RGPD.

Por tanto, cuando se apliquen tanto la base legitimadora 2.a), consentimiento del interesado, como 2.b), excepcional relevancia y gravedad para la salud pública, de la Disposición Adicional Decimoséptima de la LOPDGDD, se deberán realizar las acciones que se indican en el apartado 2.f) de la misma Disposición Adicional. En el caso del apartado 2.c), reutilización de los datos, se deberán realizar las mismas acciones que en los casos precedentes y, a su vez, se necesitará el informe previo favorable del CEI y los responsables deberán publicar la información establecida en el artículo 13 del RGPD en un lugar fácilmente accesible de la página web corporativa. Por último, para aplicar el apartado 2.d), seudonimización con fines de investigación en salud, se requerirá aplicar el protocolo que recoge el mismo apartado d), llevar a cabo las acciones que se recogen en el apartado f) y contar con el informe previo del CEI previsto en la normativa sectorial.

4.3. El tratamiento de los datos relativos a la salud con fines de investigación en salud durante la pandemia:

En el informe 0017/2020[669], la AEPD analiza los tratamiento de datos que pueden realizarse en el contexto del COVID-19. Aunque es cierto que en el citado documento se hace referencia a las letras g) e i) del RGPD, no se menciona en ningún momento el ámbito de la investigación. A su vez, como acaba de indicarse, se basa en el RGPD y no en la D.A.17ª.2 de la LOPDGDD, desaprovechando la oportunidad de realizar una interpretación nacional de las bases legitimadoras para el tratamiento de los datos relativos a la salud con fines de investigación en una situación de emergencia sanitaria.

---

[668] CIOMS y OMS., "Pautas éticas internacionales para la investigación relacionada con la salud con seres humanos", *cioms*, 2017, disponible en: https://cioms.ch/wp-content/uploads/2017/12/CIOMS-EthicalGuideline_SP_INTERIOR-FINAL.pdf *[Última consulta: 31 de julio de 2021]*

[669] AEPD. Informe jurídico núm. 0017/2020 de 12 de marzo de 2020

Las investigaciones científicas destinadas a luchar contra la pandemia se han podido amparar en el consentimiento del interesado de acuerdo a lo dispuesto en la D.A.17ª.2.a) del RGPD. De la misma manera, el consentimiento del interesado también ha servido para permitir el tratamiento de los datos personales que se ha derivado del uso de una aplicación informática para el apoyo en la gestión de la crisis sanitaria ocasionada por el COVID-19[670], aunque dicho tratamiento no se ha realizado estrictamente con fines de investigación sino para el control de la propagación de la enfermedad. Sin perjuicio de lo anterior, en el contexto de la pandemia, en la normativa española se identifican otras vías o bases mucho más sencillas y de mayor interés para los investigadores, lo cual les ha permitido evitar solicitar el consentimiento a los interesados en ciertas situaciones.

De acuerdo con lo dispuesto en la D.A.17ª.2.b), las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública[671] han podido llevar a cabo estudios científicos sin el consentimiento de los interesados, incluso manteniendo los datos de identificación del mismo. Por tanto, han podido realizar un uso secundario sin la necesidad de requerir nuevamente el consentimiento y sin realizar ni tan siquiera la seudonimización[672].

A diferencia de lo que sucede con el estado de excepción, la declaración del estado de alarma no supone, en ningún caso, ni expresa ni tácitamente, la suspensión del derecho fundamental a la protección de datos. No obstante, el citado derecho fundamental puede de ser amoldado para permitir legítimamente los tratamientos de datos personales en situaciones en las que existe una emergencia sanitaria de alcance general[673]. Los investigadores han necesitado una gran cantidad de datos clínicos de pacientes positivos que estuviesen hospitalizados o en cuarentena para extraer la información y conocimiento, y así hacer frente al COVID-19 en base al interés público. Sin embargo, los tratamientos de datos relativos a la salud con fines de investigación que se realizan

[670] La Orden SND/297/2020, de 27 de marzo (BOE núm.86 de 28 de marzo de 2020) encomendó a la Secretaría de Estado de Digitalización e Inteligencia Artificial el desarrollo de una aplicación informática que permitiera al usuario realizar una autoevaluación con base en los síntomas médicos que comunicara, acerca de la probabilidad de que estuviera infectado por el COVID-19, ofrecerle información sobre la enfermedad y consejos prácticos y recomendaciones, según la evaluación. El Ministerio de Sanidad ha sido el responsable del tratamiento de los datos personales. Como el uso de este tipo de aplicaciones ha sido voluntario, se ha exigido el consentimiento explícito del interesado para llevar a cabo el tratamiento de sus datos personales.

[671] Según lo dispuesto en el artículo 16.3 de la LBAP, la cual fue modificada por La Disposición Final 9ª de la LOPDGDD, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, han podido acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública, siempre que el acceso lo haya realizado un profesional sanitario sujeto al secreto profesional o otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.

[672] CBE., Informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de Covid-19, 28 de abril de 2020, p. 15

[673] RODRÍGUEZ AYUSO, J.F., ”Dossier cuestiones bioéticas de la pandemia covid-19”, *Revista de Bioética y Derecho*, Núm. 50, 2020, p. 358

en situaciones de emergencia sanitaria en base al interés público no pueden convertirse en prácticas habituales, la sociedad debe confiar en las autoridades públicas[674].

En este punto, cabe destacar otro tratamiento de datos relativos a la salud sin fines de investigación que se ha realizado en el contexto de la pandemia: el registro de vacunación frente a COVID-19, llevado a cabo, según el Ministerio de Sanidad[675] y, entre otros, el Departamento de Salud del Gobierno Vasco[676], en base al interés público esencial en el ámbito específico de la salud pública para la vigilancia epidemiológica. El artículo 27.2 del Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19[677], indica que el tratamiento de la información de carácter personal que se realice como consecuencia del desarrollo y aplicación del mismo tendrá por finalidad el seguimiento y vigilancia epidemiológica del COVID-19 para prevenir y evitar situaciones excepcionales de especial gravedad, atendiendo a razones de interés público esencial en el ámbito específico de la salud pública, y para la protección de intereses vitales de los afectados y de otras personas físicas al amparo de lo establecido en el RGPD.

A su vez, en base a la D.A. 17ª.2.d), los grupos de investigación, no solo enmarcados dentro del sistema sanitario y de investigación públicos, han podido realizar un uso secundario de los datos de salud, como los existentes en las historias clínicas de los pacientes atendidos por infección por COVID-19 en los centros sanitarios públicos y privados con fines de investigación científica, exigiéndose, en este caso, tanto proceder a la seudonimización de los datos desde su origen como a solicitar la autorización del correspondiente Comité de Ética de la Investigación tal y como dispone el apartado g)[678].

---

[674] En este sentido, el autor HARARI pone como ejemplo el caso hipotético de un gobierno que exige a todos los ciudadanos que usen un brazalete biométrico que monitorea la temperatura corporal y la frecuencia cardíaca las 24 horas del día. Los datos resultantes serán acumulados y analizados por algoritmos gubernamentales. Como afirma el autor, los algoritmos permitirán saber que una persona está enferma incluso antes de que ésta lo sepa, permitiendo que las cadenas de infección se acorten drásticamente e incluso que se corten por completo, deteniendo la epidemia en seco en unos días. No obstante, mediante dicha actividad, se estaría legitimando un sistema de vigilancia extremo, puesto que, incluso cuando las infecciones por coronavirus se redujeran a cero, algunos gobiernos ávidos de datos podrían argumentar que necesitan mantener los sistemas de vigilancia porque temen una segunda ola de coronavirus, o porque hay una nueva cepa de Ébola evolucionando en África central, etc. Véase al respecto: HARARI, Y.N., "The world after coronavirus", *Financial Times*, 20 de marzo de 2020, Disponible en: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75 *[Última consulta: 1 de agosto de 2021]*

[675] MINISTERIO DE SANIDAD., "Inventario de actividades de tratamiento de datos personales de las unidades que estaban integradas en el extinto ministerio de sanidad, consumo y bienestar social", *mscbs*, 23 de agosto de 2022, disponible en: https://www.mscbs.gob.es/servCiudadanos/proteccionDatos/docs/RAT_MSCBS.pdf

[676] DEPARTAMENTO DE SALUD DEL GOBIERNO VASCO., "Transparencia sobre el nuevo coronavirus (COVID-19)", *euskadi.eus*, 26 de mayo de 2021, disponible en: https://www.euskadi.eus/vacunacion/web01-a3txerto/es/ *[Última consulta: 2 de agosto de 2021]*

[677] BOE núm. 163 de 10 de junio de 2020

[678] CBE. Informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de Covid-19, *cit.*, p. 16

5. EL TRATAMIENTO DE LOS DATOS RELATIVOS A LA SALUD CON FINES DE INVESTIGACIÓN CIENTÍFICA EN ITALIA:

Tras analizar la regulación relativa al tratamiento de los datos relativos a la salud con fines de investigación tanto en el RGPD como en la LOPDGDD, y con el objetivo de identificar las diferencias que existen en este ámbito entre los distintos ordenamientos, en el presente epígrafe se estudiará el caso particular de Italia. Para ello, se indicará cuál es la normativa aplicable, cómo se regula el tratamiento de los datos relativos a la salud para la investigación médica, biomédica e epidemiológica; el tratamiento posterior de los datos personales por parte de terceros con fines estadísticos o de investigación científica; y por último, cómo se ha realizado el tratamiento de los datos relativos a la salud con fines de investigación durante la pandemia.

5.1. Normativa aplicable:

Con carácter previo a la entrada en vigor del RGPD, en Italia era de aplicación el Decreto Legislativo núm.196 de 30 de junio de 2003, denominado "Código en materia de protección de los datos personales". Posteriormente, entró en vigor el Decreto Legislativo núm. 101 de 10 de agosto de 2018 para la adaptación de la legislación nacional al RGPD.

A diferencia del legislador español, el italiano no derogó completamente el anterior Decreto Legislativo (196/2003), sino que lo modificó con el ulterior Decreto Legislativo (101/2018), logrando como resultado el "Código relativo a la protección de datos personales, que contiene disposiciones para la adaptación de la legislación nacional al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE", en adelante el Código de protección de datos personales o el Código. Es decir, el Código italiano es el resultado de la aplicación del Decreto legislativo 101/2018 al Decreto legislativo 196/2003.

El antiguo Código contenía diversos anexos. Los apartados 3 y 4 del artículo 20 del nuevo Código encomendaron al "Garante", autoridad administrativa independiente italiana de protección de datos personales, la tarea de verificar, dentro de los 90 días siguientes a su entrada en vigor, que las disposiciones contenidas en esos anexos cumplían lo dispuesto en el RGPD. En consecuencia, el Garante pretendía armonizar las antiguas normas éticas con las disposiciones del Reglamento, modificándolas e integrándolas[679].

Las disposiciones que se consideraron compatibles, rebautizadas como normas deontológicas, "*regole deontologiche*", se publicaron en el Boletín Oficial de la República Italiana ("*Gazzetta"*) y, por decreto del Ministerio de Justicia, se incluyeron

[679] MARTORANA, M., *GDPR e Decreto Legislativo 101/2018. Vademecum del profesionista: obblighi, adempimenti, strumenti di tutela,* Wolters Kluwer, Milan, 2019, pp. 51-52

posteriormente en el Anexo A del Código. Las reglas deontológicas, las cuales han de ser comprendidas como principios inherentes a sectores específicos o finalidades de tratamiento que prevén medidas y precauciones para proteger a los interesados[680], son igualmente mencionadas en el artículo 2 cuarto "*quater*" del Código, siendo su cumplimiento una condición esencial para la licitud del tratamiento de datos personales[681]. En base al artículo 2 séptimo del Código (medidas de garantía para el tratamiento de datos genéticos, biométricos y relativos a la salud), además de las normas deontológicas, se deben adoptar las medidas de garantía como, por ejemplo, la seudonimización o minimización de datos para llevar a cabo el tratamiento de dichos datos[682]. Estas medidas de garantía se eligen e introducen teniendo en cuenta los fines específicos del tratamiento en cuestión[683].

A su vez, previa a la entrada en vigor del actual Código, había multitud de Autorizaciones Generales[684] que fueron analizadas para ver si se adecuaban o no a la reforma legislativa. Mediante la disposición general n. 497 del 13 de diciembre de 2018, el Garante identificó las disposiciones compatibles con el RGPD de las Autorizaciones Generales números 1/2016 (para el tratamiento de datos sensibles en las relaciones laborales), 3/2016 (para el tratamiento de datos sensibles por asociaciones y fundaciones), 6/2016 (para el tratamiento de datos sensibles por parte de investigadores privados), 8/2016 (para el tratamiento de datos genéticos) y 9/2016 (para el tratamiento de datos personales con fines de investigación científica). Una vez identificadas las disposiciones compatibles, por medio de la disposición de 5 de junio de 2019, n. 146, el Garante emitió la "Disposición que contiene las disposiciones relativas al procesamiento de categorías particulares de datos, de conformidad con el art. 21, párrafo 1 del Decreto Legislativo 10 de agosto de 2018, n. 101"[685]. En dicha disposición, se realiza una actualización y modificación de las disposiciones contenidas en las citadas autorizaciones generales para cumplir con lo dispuesto en el RGPD. Por ende, el marco de la disciplina se completa con la disposición, ya mencionada, de 5 de junio de 2019.

El título V del Código regula el tratamiento de los datos personales en el ámbito sanitario, enfocándose en el tratamiento de los datos personales con fines de asistencia

---

[680] Ibid., p. 12

[681] CICCIA, A., Guida *al Codice Privacy. Come cambia dopo il GDPR e il D. lgs. N. 101/2018*, Wolter Kluwer, Milan, 2018, p. 48

[682] MORETTI, M., "Dati personali in Sanità e per la ricerca: i provvedimenti del Garante Privacy del quadro UE", *agendadigitale*, 12 de julio de 2019, https://www.agendadigitale.eu/sicurezza/dati-personali-in-sanita-e-per-la-ricerca-i-provvedimenti-del-garante-privacy-nel-quadro-ue/ *[Última consulta: 22 de octubre de 2021]*

[683] Artículo 2-séptimo.5 del Código

[684] Desde mediados de los años 90, mediante las Autorizaciones Generales, el Garante ha permitido el tratamiento de datos sensibles o datos judiciales en determinadas circunstancias. Por tanto, las Autorizaciones, en sentido genérico, han constituido una condición de licitud del tratamiento de datos personales. Véase al respecto: GORETTA, R., "Autorizzazioni generali dopo il GDPR, cosa cambia", *Agenda digitale*, 28 de enero de 2019, disponible en: https://www.agendadigitale.eu/sicurezza/autorizzazioni-generali-dopo-il-gdpr-cosa-cambia/ *[Última consulta: 22 de octubre de 2021]*

[685] "*Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101"*

sanitaria. En este sentido, el artículo 75 del Código dispone que el tratamiento de datos personales que se lleve a cabo con la finalidad de proteger la salud y seguridad física del interesado o de terceros o de la comunidad deberá realizarse de conformidad con los artículo 9.2.h), 9.i) y 9.3 del RGPD, así como el artículo 2 séptimo del Código, relativo a las medidas para el tratamiento de datos genéticos, biométricos y de salud, y las disposiciones específicas del sector.

En cuanto al contenido del Código de mayor interés para el presente trabajo, el título VII regula el tratamiento de datos con fines de archivo en interés público, para investigación científica o histórica o con fines estadísticos, de conformidad con el artículo 89 del reglamento. El referido título se compone de tres subgrupos: perfiles generales, tratamiento de datos con fines de archivo en interés público o para investigación histórica y el tratamiento de datos con fines estadísticos o de investigación científica. En el presente epígrafe se procederá a analizar el tercer subgrupo.

5.2. El tratamiento de los datos relativos a la salud para la investigación médica, biomédica e epidemiológica:

El tratamiento de los relativos a la salud para la investigación en salud se regula en los artículos 110 y 110bis del Código. El primero regula el tratamiento de los datos relativos a la salud para la investigación médica, biomédica e epidemiológica. En cuanto al segundo, regula el tratamiento posterior de los datos personales, incluidos los relativos a la salud, por parte de terceros con fines estadísticos o de investigación científica.

Tanto en el RGPD como en el Código se utiliza siempre el término "investigación científica" sin especificaciones ni limitaciones, abierto a todos los campos del conocimiento y la ciencia, con excepción del artículo 110 del Código que se refiere, tal y como se acaba de exponer, expresamente a la investigación médica, biomédica y epidemiológica[686]. El ámbito de aplicación del artículo 110 es la investigación médica en un sentido general, también en términos de investigación biomédica e investigación epidemiológica. Se trata de una investigación interdisciplinar en el campo de la medicina que incorpora nociones y aportes metodológicos derivados de la biología y otras disciplinas científicas, aplicándolas a la comprensión de los mecanismos fisiológicos, patológicos y farmacológicos[687]. De una simple lectura se desprende que el artículo objeto del presente análisis considera el consentimiento del interesado la "regla" para la investigación médica, biomédica y epidemiológica, indicando

[686] MARINI, P., "Dati sensibili e GDPR: il provvedimento del Garante", *Altalex*, 31 de julio de 2019, disponible en: https://www.altalex.com/documents/news/2019/07/31/dati-sensibili-gdpr-garante *[Última consulta: 23 de octubre de 2021]*

[687] BOLOGNINI, L. Y PELINO, E., *Codice della disciplina privacy*, Giuffrè Francis Lefebrve, Milan, 2019, p. 125

posteriormente las excepciones de dicha regla. Es decir, los casos en los que los datos pueden procesarse sin el consentimiento del interesado[688].

Respecto a la primera excepción, no será necesario recabar el consentimiento del interesado para el tratamiento de los datos relativos a la salud con fines de investigación científica en el ámbito sanitario, biomédico o epidemiológico cuando la investigación se lleva a cabo sobre la base de disposiciones legales o reglamentarias o del Derecho de la Unión Europea de conformidad con el artículo 9.2.j) del RGPD, o incluso en el caso en el que la investigación sea parte de un programa de investigación biomédica o sanitaria contemplado en el artículo 12-bis del Decreto Legislativo, 30 de diciembre de 1992, núm. 502, y se lleve a cabo una evaluación de impacto y una consulta previa ante el Garante de conformidad con los artículos 35 y 36 del RGPD.

Por tanto, el consentimiento no es necesario, si el procesamiento se realiza sobre la base de disposiciones legales o reglamentarias o sobre la base del artículo 9.2.j) del RGPD. En el caso de que se haga uso del artículo 9.2.j), incluido el caso en el que la investigación sea parte de un programa de investigación biomédica o sanitaria previsto de conformidad con el artículo 12bis del Decreto Legislativo 502/1992, se requiere que el responsable del tratamiento proceda, de manera preliminar, a realizar una evaluación de impacto y una consulta previa ante el Garante[689].

En cuanto a la segunda excepción, no será necesario recabar el consentimiento del interesado cuando, por motivos particulares, sea imposible o implique un esfuerzo desproporcionado informar a los interesados o se pueda imposibilitar o comprometer gravemente el logro de los fines de la investigación. La idea del legislador italiano que inspira dicha excepción es la siguiente: el consentimiento válido es el consentimiento informado, por lo tanto, en ausencia de información adecuada, no se puede contar con un consentimiento eficaz[690]. En tales casos, el tratamiento se considerará lícito solo si se ha solicitado y obtenido un dictamen motivado del Comité de Ética, así como realizado la consulta previa ante el Garante de conformidad con el artículo 36 del RGPD[691].

Llegados a este punto, es necesario exponer el contenido de la Autorización General n.9/2016, para el tratamiento de datos personales con fines de investigación científica, de 15 de diciembre de 2016 *("Autorizzazione generale al trattamento dei dati personali effettuato per scopi di ricerca scientifica*") cuyo contenido fue actualizado y modificado tras la disposición n. 146 de 5 de junio de 2019 del Garante. La citada Autorización se refiere al tratamiento de datos relativos a la salud, siempre y cuando dicho tratamiento sea indispensable para lograr los fines de la investigación, y los datos referentes a la vida sexual y origen racial y étnico, incluso sin el consentimiento de los interesados, con fines de investigación científica en los campos médico, biomédico o epidemiológico, en el cumplimiento de ciertos límites y condiciones.

---

[688] IASESSI, M., *La tutela dei dati personali in ámbito sanitario,* Giuffrè Francis Lefebrve, Milan, 2020, p. 156
[689] BOLOGNINI, L. y PELINO, E., *Codice della disciplina privacy*, *cit.*, p. 42
[690] Ibid., p. 43
[691] IASESSI, M., *La tutela dei dati personali in ámbito sanitario, cit.*, p. 156

En cuanto al primer escenario, este se refiere a la existencia de "motivos éticos imputables al hecho de que el interesado desconozca su condición sanitaria". Dentro de esta categoría se incluyen aquellas situaciones en las que otorgar información sobre el estudio a los interesados podría ocasionarles daños materiales o psicológicos, por ejemplo, estudios epidemiológicos sobre la distribución de un factor que predice o puede predecir el desarrollo de un estado de enfermedad para el que no existe tratamiento médico[692]. Por tanto, cuando una persona no sea realmente consciente de su condición sanitaria, y otorgarle dicha información pueda provocarle un daño material o psicológico, se podrá realizar el tratamiento de sus datos sin otorgarle la previa información por la existencia de motivos éticos.

En relación directa con la segunda excepción del artículo 110 del Código, el punto dos de la autorización se refiere al tratamiento de datos de interesados a los cuales no se les puede contactar para otorgarles la información requerida por el RGPD por la existencia de alguno de los dos motivos contemplados en la autorización: motivos éticos y motivos de imposibilidad organizativa.

Así, el segundo escenario alude a las razones de imposibilidad organizativa atribuible a que el número estimado de interesados que no puedan ser contactados para informarles, en comparación con el total de sujetos que se pretenden involucrar en la investigación sea muchísimo menor, y produciría importantes consecuencias para el estudio en términos de alteración de los resultados; teniendo en cuenta, en particular, los criterios de inclusión previstos por el estudio, el número estadístico de la muestra elegida, así como el período de tiempo transcurrido desde el momento en que los datos relativos a los interesados se recopilaron originalmente (por ejemplo, en los casos en que el estudio se refiera a personas con patologías con alta incidencia de mortalidad o en fase terminal de la enfermedad).

Dentro de este contexto también es necesario incluir el tratamiento de los datos de personas que, después de realizar todos los esfuerzos razonables para contactarlos (a través de la verificación del estado de vida, la consulta de los datos reportados en la documentación clínica, así como la adquisición de datos de contacto en el registro de población asistida o residente), se clasifiquen como fallecidos o no contactables[693].

En consecuencia, el artículo 110 del Código reproduce las dos excepciones previstas anteriormente por la Autorización 9/2016. Esto es, aunque hasta el 2018 dichas excepciones fuesen únicamente recogidas por la Autorización, ahora se encuentran igualmente en el Código. Por tanto, en cierto sentido, es como si estas excepciones se hubieran convertido en ley. Sin embargo, técnicamente el artículo 110 se aplica directamente.

[692] CASSANO, G; COLAROCCO, V; GALLUS, G.B. y M, F.P., *Il proceso di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018 n.101*, Giufrè Francis Lefebvre, Milan, 2018, p. 333
[693] GUARDA. P., "Art. 110", en D'ORAZIO, R; FINOCCHIARO, G; POLLICINO, O. y RESTA, G., *Codice della privacy e data protection*, Giuffrè Francis Lefebvre, Milan, 2021, p. 1375-1376

Sin perjuicio de lo anterior, tras la disposición n. 146 de 5 de junio de 2019 del Garante, se ha introducido una tercera excepción, aplicable cuando existan razones de salud atribuibles a la gravedad del estado clínico en el que se encuentra el interesado. Es decir, la presente excepción será aplicada cuando una persona no puede comprender la información proporcionada y dar válidamente su consentimiento para el tratamiento de sus datos personales. En tales casos, el estudio debe tener como objetivo mejorar el estado clínico en el que se encuentra el interesado. Además, es necesario demostrar que los fines del estudio no pueden lograrse mediante el procesamiento de datos referentes a personas capaces de comprender la información proporcionada y dar válidamente su consentimiento o con otros métodos de investigación. Esto, teniendo en cuenta, en particular, los criterios de inclusión previstos por el estudio, los métodos de contratación, el número estadístico de la muestra elegida, así como la fiabilidad de los resultados que se pueden alcanzar en relación con los fines específicos de el estudio. La información sobre el tratamiento de los datos deberá ser facilitada al interesado tan pronto como su condición de salud lo permita, pudiendo, este último, ejercitar los derechos previstos en la normativa[694].

Una de las principales dificultades a la que se enfrentan los investigadores está relacionada con la necesidad de la recopilación de los de carácter sanitario del paciente cuyo estado de conciencia parece estar ausente en situaciones de urgencia en las que el interesado se encuentra en peligro de muerte por un trauma grave ante el cual es imposible obtener un consentimiento válido del paciente. Se trata de condiciones que requieren intervención médica inmediata y en presencia de lo cual es difícil encontrar en poco tiempo al representante legal del paciente, precisamente porque muchas veces no están inmediatamente disponibles o rastreables[695].

A modo de ejemplo, cuando sea necesario recabar los datos del paciente (el sujeto directamente interesado del tratamiento de datos de carácter sanitario) que accede al servicio de urgencias habiendo sufrido un trauma o una lesión que comprometa significativamente su condición de salud, y no se encuentra en las condiciones óptimas y necesarias para que pueda otorgar un consentimiento del interesado válido para inscribirse en un determinado proyecto, podrá aplicarse la presente excepción. En esta circunstancia, las condiciones físicas y/o aspectos psicológicos del paciente, y la muy limitada disponibilidad de tiempo, no permiten la recogida de un consentimiento válido. Si el paciente vuelve a estar consciente, éste debe en todo caso ser completamente informado sobre los métodos y propósitos del procesamiento de sus datos salud con fines de investigación, para que pueda conscientemente decidir si quiere seguir en el mismo o no[696]. Independientemente del tipo de investigación científica que se pretenda realizar, cuando es muy difícil o imposible recabar el consentimiento del interesado, el

[694] MARINI, P., "Dati sensibili e GDPR: il provvedimento del Garante", *cit.*
[695] BUSCA, N., "Il trattamento dei dati sanitari nell´ambito della ricerca e della sperimentazione clínica", *Rivista responsabilita medica*, Núm. 9, 2020, p. 4
[696] Ibid., p. 5

protocolo del proyecto de investigación deberá en todo caso ser previamente aprobado por el Comité de Ética competente y realizar una consulta ante el Garante.

En relación directa con lo antedicho, para que una de estas tres excepción sea aplicable, los motivos deben ser considerados completamente particulares o excepcionales y estar documentados en el proyecto de investigación[697]. Así, el programa de investigación debe desarrollar ampliamente el por qué, tener una opinión favorable del Comité de Ética territorial y realizar una consulta previa al Garante en el sentido del artículo 36 del RGPD[698]. La última parte del artículo 110.1 del Código aporta garantías adicionales cuya justificación parece ser la de llenar la falta de información. El legislador italiano ha tratado de que la falta de información se compense obligando al responsable del tratamiento a adoptar las medidas de protección adecuadas, sometiendo el programa de investigación a un dictamen motivado y obligando a realizar una consulta previa. En consecuencia, las citadas garantías están destinadas a reequilibrar el desequilibrio resultante[699].

Según se recoge en el apartado 5.7 de la disposición n. 146 de 5 de junio de 2019, (apartado 6 de la Autorización 9/2016), sin perjuicio de la obligación de adoptar las medidas mínimas de seguridad previstas por el Código, el responsable del tratamiento deberá adoptar medidas específicas y técnicas para incrementar el nivel de seguridad de los datos tratados para la ejecución del estudio. Tanto en la fase de almacenamiento o archivo de datos como en la fase posterior de tratamiento, así como en la fase posterior de transmisión de datos al promotor o colaborador se deben adoptar cuatro tipos de medidas.

Dentro del primer grupo se encuentran las medidas adecuadas para garantizar la calidad de los datos y la correcta atribución a los interesados. En el segundo grupo se identifican las medidas adecuadas para garantizar la protección de los datos de la firma frente a los riesgos de acceso no autorizado a los datos, robo o pérdida parcial o total de los medios de almacenamiento o de los sistemas de procesamiento portátiles o fijos (por ejemplo, mediante la aplicación parcial o total de tecnologías criptográficas a los sistemas de archivos o bases de datos, o mediante la adopción de otras medidas que hagan que los datos sean ininteligibles para sujetos no autorizados) en las operaciones de registro y archivo de datos.

El tercer grupo es el relativo a los canales de transmisión protegidos, teniendo en cuenta el estado de la tecnología, en los casos en que sea necesario comunicar los datos recopilados como parte del estudio a una base de datos centralizada donde se almacenan y archivan o a un promotor o sujetos externos de los cuales el mismo promotor utiliza

[697] MUIÀ P.P., "Le prescrizioni del Garante privacy relative al trattamento di dati personali effettuato per scopi di ricerca scientifica", *Diritto.it*, 12 de septiembre de 2019, disponible en: https://www.diritto.it/le-prescrizioni-del-garante-privacy-relative-al-trattamento-di-dati-personali-effettuato-per-scopi-di-ricerca-scientifica/ *[Última consulta: 26 de octubre de 2021]*

[698] PETRINI, C., *Utilizzo di dati nella ricerca biomédica e negli interventi di sanità pubblica in tempo di Covid-19: alcune implicazioni di ética*, Invalsi, Roma, 2021, p. 16

[699] BOLOGNINI, L. y PELINO, E., *Codice della disciplina privacy*, *cit.*, p. 125

para la realización del estudio. El cuarto grupo se refiere a las técnicas de etiquetado, en la conservación y transmisión de muestras biológicas, mediante códigos de identificación, u otras soluciones que, considerando el número de muestras utilizadas, las hagan no directamente atribuibles a los interesados, permitiendo su identificación solo en caso de necesidad.

Por último, con referencia específica a las operaciones de procesamiento de los datos del estudio almacenados en una base de datos centralizada, es necesario adoptar sistemas de autenticación y autorización adecuados para los designados según los roles y las necesidades de acceso y procesamiento, utilizando credenciales de validez limitada durante la duración del estudio y desactivándolas al final del mismo; procedimientos para la verificación periódica de la calidad y coherencia de las credenciales de autenticación y los perfiles de autorización asignados a los procesadores de datos; y sistemas de registro de auditoría para controlar el acceso a la base de datos y detectar anomalías.

5.3. El tratamiento posterior de los datos personales por parte de terceros con fines estadísticos o de investigación científica:

En lo referente al tratamiento posterior de los datos por parte de terceros con fines estadísticos o de investigación científica que recoge el artículo 110 bis del Código, el Garante de protección de datos personales puede autorizar el procesamiento posterior de datos personales, incluidos los de tratamientos especiales a que se refiere el artículo 9 del RGPD como los datos relativos a la salud, con fines de investigación científica o con fines estadísticos a terceros que realizan principalmente estas actividades cuando, debido por motivos particulares, es imposible informar a los interesados o supone un esfuerzo desproporcionado, o es probable que haga imposible o afecte gravemente al logro de los objetivos de la investigación, y siempre y cuando se tomen medidas apropiadas para proteger los derechos, libertades e intereses legítimos del interesado, de conformidad con el artículo 89 del RGPD, incluidas las formas preventivas de minimización y anonimización de datos[700].

En consecuencia, no se requiere el consentimiento del interesado para el tratamiento posterior de los datos personales con fines de investigación científica cuando se cumplan tres condiciones: el tratamiento lo lleva a cabo un tercero que realiza principalmente actividades de investigación científica; es imposible o implica un esfuerzo desproporcionado informar a las partes interesadas o se corre el riesgo de que la investigación se vea perjudicada gravemente, y el Garante ha otorgado una

[700] PENASA, S. y TOMASI, M., "The Italian way for research biobanks after GDPR: hybrid normative solutions to balance the protection of individuals and freedom of research", en SLOKENBERGA, S., TZORTZATOU, O., y REICHEL, J., *GDPR and biobaking: individual rights, public interest and research regulation across Europe*, Springer, Suiza, 2021, p. 318

autorización la cual está sujeta a la adopción de las medidas apropiadas de conformidad con el artículo 89 del RGPD[701].

La hipótesis regida por el artículo 110bis del Código es diferente al del artículo anterior, que se refería al tratamiento específico de datos relacionados con la salud con fines de investigación científica en los ámbitos médico, biomédico o epidemiológico[702]. El artículo 110 bis recoge el tratamiento posterior de datos por un tercero. Esta norma, cuyo título remite nuevamente a la noción de "investigación científica" y por tanto se aplica a un ámbito más amplio, establece que, cuando la obligación de informar a los interesados sea imposible o suponga un esfuerzo proporcionado o conlleve riesgos que pongan en peligro la investigación, el tratamiento podrá realizarse sin el consentimiento del interesado previa solicitud de autorización del Garante[703]. Por ello, es necesario advertir de que el propósito de la investigación científica tiene un alcance mucho más amplio que el mero sector médico, como es el caso del artículo anterior[704]. Las dos disposiciones, a pesar de la proximidad de su ubicación, tienen diferentes objetivos. El artículo 110bis se refiere a cualquier tipo de datos personales, por lo tanto, no solo datos sensibles, sino también "comunes"[705].

El artículo 110bis forma parte del contexto más general del tratamiento de datos personales con fines de investigación científica, abarcando los tratamientos especiales a que se refiere el artículo 9 del RGPD, que tiene su base jurídica en el artículo 89 del RGPD. Merece ser subrayado que la justificación de esta disposición está en la voluntad del legislador de brindar garantías para conciliar, por un lado, la necesidad de hacer avanzar la ciencia favoreciendo la investigación y la evolución tecnológica, y por otro lado, proteger el derecho a la protección de datos personales los sujetos involucrados. El objetivo que se persigue es, por tanto, permitir el uso posterior de los datos con fines de investigación científica, incluso sin el consentimiento previo de las partes interesadas, aplicando garantías y salvaguardias adecuadas.

Las palabras "tercero", "razones particulares" y el adverbio "principalmente" introducidos en primer párrafo del artículo objeto del presente análisis requieren una aclaración específica. La noción de tercero no está definida por el RGPD, excepto para la regulación de las relaciones con un tercer país o una organización internacional a la que es posible una transferencia de datos personales[706], ni en el Código. Sin embargo, parece metodológicamente correcto conectarla con la definición proporcionada por el art. 4.10 del RGPD, es decir: "persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la

[701] MARTORANA, M., *GDPR e Decreto Legislativo 101/2018. Vademecum del profesionista: obblighi, adempimenti, strumenti di tutela*, cit., p. 53
[702] BOTTARI, C., *La salute del futuro: prospettive e nuove sfide del diritto sanitario*, Bolonia University Press, Bolonia, 2020, p. 80
[703] IASESSI, M., *La tutela dei dati personali in ámbito sanitario, cit*., p. 156
[704] BOLOGNINI, L. y PELINO, E., *Codice privacy: Tutte le novità del D.LGS. 101/2018*, Giuffrè Francis Lefebrve, Milan, 2018, p. 43
[705] BOLOGNINI, L. y PELINO, E., *Codice della disciplina privacy, cit.*, p. 157
[706] BOTTARI, C., *La salute del futuro: prospettive e nuove sfide del diritto sanitario, cit.*, p. 79

autoridad directa del responsable o del encargado". En esencia, por "tercero" debe entenderse un responsable del tratamiento distinto a aquél que realizó el tratamiento inicial. Con el enfoque sistemático análogo, cabe entender el adverbio "principalmente" en el mismo sentido que se le da a la noción de "actividades principales". Finalmente, "razones particulares" sigue siendo una expresión indeterminada que solo permite especificar que, al tratarse de situaciones especiales o peculiares, deben reflejar el caso concreto y no referirse a situaciones generales[707].

En la práctica, se trata de la posibilidad de que estos sujetos (universidades, centros de investigación, fundaciones, etc.) soliciten el acceso a los datos recogidos y almacenados por otro responsable del tratamiento para utilizarlos con fines de investigación, cuando por motivos particulares, informar a los interesados es imposible o supone un esfuerzo desproporcionado, o corre el riesgo de imposibilitar o comprometer gravemente la consecución de los fines de la investigación. Por lo tanto, estos terceros tendrán la posibilidad de seguir utilizando los datos, pero solo a condición de que se tomen las medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, de acuerdo con el artículo 89 RGPD. Cualquier proyecto de reutilización de datos debe demostrar que las medidas que adopta son adecuadas y documentadas[708].

El apartado 1 del artículo 110bis del Código se refiere al procesamiento de datos personales para distintos fines de aquellos para los que fueron recopilados inicialmente los datos personales. Este tratamiento posterior solo es posible si se cumplen las condiciones de imposibilidad o desproporcionalidad antes mencionadas, y siempre y cuando se apliquen medidas adecuadas para proteger a los interesados en cumplimiento del artículo 89 del RGPD, incluyendo la minimización y anonimización de datos. Así, a diferencia de la Disposición Adicional Decimoséptima de la LOPDGDD, en la normativa italiana se exige la anonimización de los datos. Con referencia a esto último, la crítica es que a nivel teórico la información anónima está fuera del ámbito de aplicación de la normativa de protección de datos personales. También ha de tenerse en cuenta que en los escenarios actuales de la investigación científica y en el contexto del fenómeno del Big data es difícil poder decir con certeza que un conjunto de información ha sido completamente anonimizado y por tanto privado de cualquier referencia que permite incluso indirectamente la identificación de una persona.

La decisión sobre la solicitud de autorización a que se refiere el primer párrafo del artículo 110bis debe ser comunicada por el Garante en el plazo de 45 días, y el segundo párrafo confiere a la inacción de la administración pública el significado de respuesta negativa. Si, por el contrario, se expide la autorización, la disposición o las medidas ulteriores que se adopten tras las verificaciones establecen las condiciones y medidas necesarias para asegurar las garantías adecuadas para la protección de los interesados, incluso en cuanto a su seguridad. El Garante también tiene derecho a adoptar, incluso de oficio, medidas generales, potencialmente en relación con determinadas categorías de responsables del tratamiento y tratamientos, con las que se establecen las condiciones de

[707] BOLOGNINI, L. y PELINO, E., *Codice della disciplina privacy*, *cit.*, p. 157
[708] GUARDA. P., "Art. 110", *cit.*, p. 1379

tratamiento posterior y se prescriben las medidas que se puedan conocer de tales medidas generales desde su publicación en el Boletín Oficial de la República Italiana. Este instrumento de autorización general ha de comprenderse como un conjunto de normas generales y preventivas para categorías de titulares y tratamientos[709].

El procesamiento posterior de datos se deja en manos de una autorización previa del Garante. Así, se ha afirmado que la elección del legislador italiano parece ir en contra de la tendencia, si no en contraste, de la implantada a nivel europeo. Los artículos 9 y 89 del RGPD subordinan el tratamiento de los datos relativos a la salud con fines de investigación a la adopción de medidas técnicas y organizativas dirigidas a asegurar el cumplimiento del principio de minimización. La elección de diferir la posibilidad de reutilización de los datos relativos a la salud a la autorización expresa del Garante se convierte en un requisito adicional, no previsto a nivel europeo, y como tal susceptible de ser considerado incompatible con la legislación comunitaria, aunque es cierto que el artículo 9.4 del RGPD permite a los estados miembros introducir condiciones adicionales, incluidas limitaciones, con referencia a datos genéticos, biométricos y relacionados con la salud. El requisito de que el Garante lleve a cabo esta actividad de control y verificación en solo cuarenta y cinco días también parece en algunos aspectos demasiado pretencioso. El riesgo real que conlleva dicha disposición es que las solicitudes de autorización puedan ser rechazadas no tanto por razones de mérito, como por la imposibilidad objetiva de evaluarlas en detalle dentro del plazo señalado, considerando, finalmente, la peculiaridad de introducir una forma de "silencio negativo", en claro contraste con los últimos enfoques del derecho administrativo. Para remediar la posible sobrecarga de solicitudes de autorización por parte del Garante, el tercer párrafo establece que este último podrá utilizar la herramienta de las categorías de titulares y tratamientos, con el fin de establecer las condiciones y medidas de garantía. La introducción de esta herramienta tiene el objetivo de permitir gestionar de forma automática y preventiva gran parte de las solicitudes de acceso y uso de datos[710].

La descrita facultad de autorización del Garante al que se refiere el punto 2 del artículo 110bis plantea cuestiones críticas, dado que no está claro por qué el procesamiento con fines de investigación científica está sujeto a una disciplina decididamente más severa que la prevista para la investigación médica. En el primero caso se requiere una autorización al Garante sometido al mecanismo de rechazo silencioso, en el segundo una solicitud de opinión al Garante de conformidad con el artículo 36 del RGPD. En palabras de BOLOGNINI, este cambio legislativo corre el riesgo de resultar dañino, puesto que, por una parte, se prevé una autorización del Garante para el *uso secundario* de los datos con fines de investigación científica, cuando en cambio el RGPD va en una dirección contraria (artículos 33, 50, 89 y 159)**.** Por otra parte, en el artículo 110bis se establece que el Garante autoriza el uso de los datos a condición de que, entre otras cosas, también sean anonimizados, y no solo minimizados en su tratamiento. Según el

[709] CASSANO, G; COLAROCCO, V; GALLUS, G.B. y M, F.P., *Il proceso di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018 n.101*, *cit.*, p. 3339
[710] GUARDA. P., "Art. 110", *cit.*, pp. 1380-1381

autor, es un poco como decir que el Garante tendrá competencia para autorizar aquello sobre lo que no tiene competencia (el procesamiento de datos anonimizados)[711].

A su vez, el artículo 110bis solo recoge la exigencia de solicitar la autorización al Garante, no requiriendo el dictamen del Comité de Ética. En el artículo 110 del Código se introduce el requisito de solicitar el dictamen del Comité de Ética para que el propio responsable del tratamiento pueda reutilizar los datos. Sin embargo, en el artículo 110bis, no se requiere dicho dictamen cuando la reutilización de los datos la realiza un tercero, siendo este hecho realmente criticable. En otras palabras, desde el punto de vista del derecho a la protección de datos personales, en Italia la obligación de contar con una opinión favorable del Comité de Ética se prevé únicamente en el artículo 110 del Código. Sin perjuicio de lo anterior, aunque esta obligación no esté recogida en el artículo 110bis del Código, los proyectos de investigación requieren la obtención de una opinión favorable del Comité de Ética.

Para concluir, el cuarto párrafo indica que el uso posterior de los datos clínicos con fines de investigación está expresamente permitido ya que la actividad asistencial que realizan los institutos mencionados por el legislador tiene un carácter instrumental respecto a la propia investigación, sin perjuicio del cumplimiento de las condiciones previstas en el artículo 89 del RGPD. La excepción, naturalmente, no debe entenderse como una norma ad hoc de salvación, sino que se presta a extenderse, en la medida de lo posible, a todos los sujetos del ordenamiento jurídico a los que ha hecho explícito el legislador, potenciando así el sentido "instrumental" de la investigación con respecto a la actividad típica que se realiza[712].

5.4. El tratamiento de los datos relativos a la salud con fines de investigación en salud durante la pandemia:

El artículo 14 del Decreto de ley 14/2020 de 9 de marzo del 2020, relativo a las disposiciones urgentes para el fortalecimiento del Servicio Nacional de Salud en relación a la emergencia COVID-19 ("*Disposizioni urgenti per il potenziamento del Servizio sanitario nazionale in relazione all'emergenza COVID-19*"), recoge que los datos personales, comunes y sensibles, entre los cuales se identifican los datos relativos a la salud, pueden ser procesados y distribuidos entre los sujetos designados por la normativa. Dichos datos pueden ser comunicados a otros sujetos públicos y privados. A su vez, se indica que el tratamiento de los datos personales debe llevarse a cabo en cumplimiento de los principios a que se refiere el artículo 5 del RGPD[713].

[711] BOLOGNINI, L., "GDPR, come l´Italia minaccia la ricerca scientifica", *agendadigitale*, 6 de diciembre de 2017, disponible en: https://www.agendadigitale.eu/sicurezza/codice-privacy-una-tagliola-italiana-in-contrasto-con-il-gdpr/ *[Última consulta: 12 de noviembre de 2021]*

[712] BOLOGNINI, L. y PELINO, E., *Codice della disciplina privacy*, *cit.*, p. 158

[713] GRUPO DI LAVORO ISS BIOETICA COVID-19., Sorveglianza territoriale e tutela della salute pubblica: alcuni aspetti ético-giuridici, (Rapporto ISS COVID-19 n.34/2020), 25 de mayo 2020, p. 9

En particular, de conformidad con los artículos 9.2 letras g), h) e i) del RGPD, ciertos sujetos involucrados en la lucha contra la emergencia COVID-19 (incluido el Servicio Nacional de Protección Civil, las oficinas del Ministerio de Salud y el Instituto Superior de Salud) también pueden procesar datos personales que sean necesarios para el desempeño de las funciones que les son asignadas en la gestión de la emergencia. Igualmente, se prevé la posibilidad de que tales datos personales sean "comunicados" a diferentes sujetos, pero solo en los casos en los que la comunicación o difusión sea imprescindible para la gestión de la emergencia. Según se indica en el último párrafo del artículo objeto de análisis, una vez cesado el estado de emergencia, se deben tomar las medidas adecuadas para que el tratamiento de datos personales realizado en el contexto de la emergencia vuelva al ámbito de las competencias y normas ordinarias. En este sentido, una vez que haya cesado la emergencia, y por lo tanto se haya alcanzado el propósito del procesamiento, la cantidad de información recopilada no podrá, en ausencia de una base legal adicional que justifique su procesamiento, ser convertida para satisfacer otros propósitos[714].

Respecto al Decreto ley 18/2020 de 17 de marzo de 2020 relativo al fortalecimiento de medidas del Servicio Nacional de Salud y apoyo económico a familias, trabajadores y empresas vinculadas a la emergencia epidemiológica del COVID-19 ("*Misure di potenziamento del Servizio sanitario nazionale e di sostegno economico per famiglie, lavoratori e imprese connesse all'emergenza epidemiologica da COVID-19*"), en su artículo 17 se recogen las disposiciones urgentes sobre pruebas de medicamentos y dispositivos médicos para la emergencia epidemiológica del COVID. Más concretamente, el citado artículo indica que limitado al período del estado de emergencia, y sin perjuicio de las disposiciones vigentes en materia de ensayos clínicos de medicamentos y productos sanitarios, para mejorar las habilidades de coordinación y análisis de la evidencia científica disponible, se confía a AIFA (Agencia Italia del Fármaco) la posibilidad de acceder a todos los datos de los estudios experimentales y de los usos compasivos de pacientes con COVID-19. Es decir, este artículo se refiere a la posibilidad que otorga la ley a AIFA de procesar los datos de los ensayos de medicamentos y dispositivos médicos de los pacientes con Covid-19. Dado el carácter excepcional de la medida, la duración de estas intervenciones debe estar estrictamente ligada a la persistencia de las necesidades relacionadas con la gestión de la emergencia[715].

El permiso que se le otorga a AIFA es nuevamente citado en el artículo 40 del Decreto ley 23/2020 de 8 de abril relativo a las Medidas urgentes en materia de acceso al crédito y obligaciones tributarias de las empresas, competencias especiales en sectores estratégicos, así como intervenciones en el ámbito de la salud y el trabajo, ampliación de plazos administrativos y procesales ("*Misure urgenti in materia di accesso al credito e di adempimenti fiscali per le imprese, di poteri speciali nei settori strategici, nonche'*

[714] MICOZZI, F. P., "Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il legalmente consentito", *BioLaw Journal-Rivista di BioDiritto*, Núm especial. 1, 2020, p. 627
[715] RUFO, L., "Le ricerche scientifiche durante l'emergenza sanitaria (il covid-19). Quale base giuridica per l'arruolamento dei pazienti", *BioLaw Journal-Rivista di BioDiritto*, Núm especial. 1, 2020, p. 431

interventi in materia di salute e lavoro, di proroga di termini amministrativi e processuali") y en el artículo 40 de la posterior ley 40/2020 de 5 de junio de Conversión en ley, con modificaciones, del decreto-ley 8 de abril de 2020, n. 23, que contiene medidas urgentes en materia de acceso al crédito y obligaciones tributarias de las empresas, competencias especiales en sectores estratégicos, así como intervenciones en el ámbito de la salud y el trabajo, ampliación de plazos administrativos y procesales ("*Conversione in legge, con con modificazioni, del decreto-legge 8 aprile 2020, n. 23, recante misure urgenti in materia di accesso al credito e di adempimenti fiscali per le imprese, di poteri speciali nei settori strategici, nonche' interventi in materia di salute e lavoro, di proroga di termini amministrativi e processuali"*).

Durante la pandemia del Covid-19, la urgente necesidad de obtener rápidamente resultados científicos útiles para contrarrestar la propagación del virus ha llevado a la Autoridad Garante a introducir una derogación parcial del artículo 110 del Código a través de la publicación de preguntas frecuentes relacionadas con el procesamiento de datos en el ámbito de los ensayos clínicos e investigación médica en el contexto de la emergencia sanitaria.

Como norma general, los promotores y los centros pueden procesar datos personales, incluidos los relacionados con la salud de los pacientes con Covid-19 para la realización de ensayos clínicos de medicamentos (por ejemplo, ensayos clínicos experimentales sobre medicamentos de fase I, II, III y IV, estudios observacionales sobre medicamentos y programas de uso terapéutico compasivo), estrictamente necesarios para combatir y estudiar la pandemia en curso, con el consentimiento de los interesados, o en base a otra base legal, de conformidad con el artículo 9.2 del RGPD.

Si por razones específicas y comprobadas no es posible obtener el consentimiento del interesado para el procesamiento de datos personales, o este acto puede comprometer seriamente el resultado exitoso de la investigación, los responsables del tratamiento no están obligados, en virtud de la legislación relativa en esta fase de emergencia, a la previa presentación del proyecto de investigación, así como a realizar la correspondiente evaluación de impacto y la consulta previa del Garante de conformidad con el artículo 110 del Código. Así, los responsables del tratamiento podrán realizar tratamientos de datos que se refieran exclusivamente a estudios experimentales y usos compasivos de medicamentos de uso humano, para el tratamiento y prevención del virus Covid-19, al amparo de la legislación relativa a esta fase de emergencia, sin ser obligada a la previa presentación del proyecto de investigación, la correspondiente evaluación de impacto y la consulta previa del Garante[716].

Una interpretación estrictamente literal de la excepción podría hacer creer que, ante la imposibilidad de obtener el consentimiento, los promotores de un estudio observacional deben presentar el proyecto de investigación y la evaluación de impacto a la consulta

[716] RIZZO, M.L., "Ricerca scientifica e Covid-19: Le basi giuridiche per trattare i dati dei pazienti per un utilizzo secondario", *Riskmanagemente360*, 2 de septiembre de 2020, disponible en: https://www.riskmanagement360.it/compliance/ricerca-scientifica-e-covid-19-le-basi-giuridiche-per-trattare-i-dati-dei-pazienti-per-un-utilizzo-secondario/ *[Última consulta: 15 de noviembre de 2021]*

previa del Garante, mientras que los promotores de un estudio clínico de carácter intervencionista estarían exentos. No obstante, esta interpretación no tiene ningún fundamento, puesto que se estaría otorgando una exención exclusivamente a los estudios intervencionistas, los cuales tienen mayor efecto en la vida de los participantes que los estudios observacionales.

El adverbio "exclusivamente" del enunciado "datos personales que conciernen exclusivamente a estudios experimentales y usos compasivos de medicamentos de uso humano, para el tratamiento y prevención del virus COVID-19", se refiere a la finalidad de **"**tratamiento y prevención del virus COVID-19**"**, por lo que se adopta un régimen de exención[717] (eliminando la necesidad de la evaluación preventiva del Garante) para todos los estudios (intervencionistas y observacionales) que tengan el objetivo de realizar un tratamiento y prevención del virus COVID-19. Por tanto, el proyecto tendrá que pasar por el Comité Ético, pero no por el Garante.

En conclusión, es razonable suponer que los estudios observacionales también disfrutan de un régimen de exención durante toda la duración de la emergencia Covid-19. Al mismo tiempo, es necesaria una intervención aclaratoria por parte del mismo Garante, lo que eliminaría los márgenes de incertidumbre residuales que pueden representar un obstáculo significativo para la realización de las actividades de investigación científica[718].

En este sentido, el Ministerio de Salud Italiano, aprobó una convocatoria para invitar a los Institutos Científicos a presentar proyectos de investigación médica financiados con fondos para la investigación en curso del IRCCS ("*Istituto di Ricovero e Cura a Carattere Scientifico*" o Instituto de Hospitalización y Atención de carácter Científico), orientada a mejorar el conocimiento de la pandemia, contribuyendo a un manejo clínico más eficiente de los pacientes contagiados y aumentando la efectividad de los tratamientos terapéuticos a disposición de las estructuras del Servicio Nacional de Salud. El tratamiento de datos personales de carácter sanitario que lleven a cabo los beneficiarios de los fondos del IRCCS antes mencionados podrá realizarse sin el consentimiento de los interesados, por corresponder a las funciones de importante interés público[719].

[717] Como bien indica el Grupo de trabajo de Bioética del Instituto Superior de Sanidad, las excepciones relativas a la normativa de protección de datos personales que han sido introducidas para la lucha contra el virus están intrínsecamente vinculadas al estado de emergencia, debiendo ser eliminadas tan pronto como termine la crisis. Véase al respecto: GRUPPO DI LAVORO ISS BIOETICA COVID-19., Protezione dei dati personali nell´emergenza COVID-19, (Rapporto ISS COVID-19 n.42/2020), 28 de mayo 2020, p. 20

[718] GRUPPO DI LAVORO ISS BIOETICA COVID-19., Etica della ricerca durante la pandemia di COVID-19: studi osservazionali e in particolare epidemiologici, (Rapporto ISS COVID-19 n.42/2020), 29 de mayo 2020, p. 14

[719] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI., "Faq", *garanteprivacy,* 2021, disponible en: https://www.garanteprivacy.it/temi/coronavirus/faq *[Última consulta: 17 de noviembre de 2021]*

Por otra parte, en el contexto de la pandemia se ha realizado un tratamiento de datos sinfines de investigación que cobra especial interés por las bases legales utilizadas, y el posible uso de los datos que puede realizarse con fines de investigación. Se trata del tratamiento de datos personales realizado con el fin de alertar a las personas que han entrado en contacto cercano con sujetos que dieron positivo y proteger su salud a través de las medidas de prevención previstas en el contexto de las medidas de salud pública vinculadas a la emergencia COVID-19, en base al artículo 6 del Decreto Ley 28/2020 de 30 de abril sobre las medidas urgentes para la funcionalidad de los sistemas de interceptación de conversaciones y comunicaciones, nuevas medidas urgentes en relación con el sistema penitenciario, así como disposiciones complementarias y de coordinación en el ámbito de la justicia civil, administrativa y contable y medidas urgentes para la implantación del sistema de Alerta por COVID-19 ("*Misure urgenti per la funzionalita' dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonche' disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19*"), se creó una plataforma nacional única, la App "Immuni"[720], para la gestión del sistema de alerta para los sujetos que, a tal efecto, hayan instalado de forma voluntaria una aplicación específica en su teléfono móvil, siendo el responsable del tratamiento de los datos personales el Ministerio de Salud italiano.

La aplicación para el seguimiento digital de los contactos de los contagiados se rige por el artículo 6 del Decreto Ley. La norma representa un prerrequisito legal adecuado para la introducción de esta medida de salud pública y cumple con los artículos 6.1.e) y 9.2.g) del RGPD y, en particular el artículo 9.2.i) del RGPD y los artículos 2ter y 2sexies del Código. El Ministerio de Salud italiano realizó la evaluación de impacto requerida por el artículo 35 del RGPD y el Garante autorizó posteriormente el tratamiento[721].

Aunque la creación de dicha aplicación se base principalmente en el interés público, la adhesión al sistema de alerta debe ser el resultado de una elección verdaderamente libre por parte del interesado, que debe estar adecuadamente informado y debe poder confiar en la transparencia del tratamiento. La adhesión voluntaria del interesado está asegurada en todas las etapas del tratamiento que realiza el Ministerio de Salud, tal y como reiteró

[720] Immuni es la aplicación móvil notificación de exposición del Gobierno italiano, realizada por el Comisionado Especial para la emergencia COVID-19 (Presidencia del Consejo de Ministros), en colaboración con el Ministerio de Salud y el Ministerio de Innovación Tecnológica y Digitalización. La mencionada aplicación cuenta con un sistema de notificación de exposición para ayudar a alertar a los usuarios potencialmente positivos al SARS-CoV-2 en una etapa temprana. Este sistema realiza un seguimiento del contacto entre los usuarios de Immuni, y cuando un usuario da positivo por SARS-CoV-2, la aplicación utiliza este sistema para notificar a otros usuarios en riesgo. El sistema se basa en Bluetooth Low Energy y no utiliza ningún dato de geolocalización. En consencuencia, si bien la aplicación sabe que tuvo lugar el contacto con un usuario infectado, cuánto duró y puede estimar la distancia que separó a los dos usuarios, no puede decir dónde tuvo lugar el contacto, ni las identidades de los involucrados. IMMUNI., "Cos'è Immuni?", *immuni.italia*, disponible en: https://www.immuni.italia.it/faq.html *[Última consulta: 19 de noviembre de 2021]*

[721] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI., "Faq", *cit.*

el Garante tanto en el dictamen sobre la norma de 29 de abril de 2020 y en la autorización de 1 de junio de 2020 de la aplicación Immuni. Las aplicaciones móviles orientadas a brindar servicios distintos a la telemedicina o en cualquier caso no estrictamente necesarias para el tratamiento (como las aplicaciones informativas o las aplicaciones de recogida de información sobre estado de salud de la población de un territorio determinado), que implican el tratamiento de datos personales, pueden ser utilizados solo con el consentimiento libre, específico, explícito e informado del interesado según se recoge en la disposición n. 9091942 de 7 de marzo de 2019. No existe la obligación legal de que los ciudadanos se sometan al "*contact traicing*" ya sea directamente, a través de una disposición que lo haga explícito, o indirectamente, fomentando su uso. La cancelación de datos debe realizarse en un plazo razonable respecto a la necesidad de control de la epidemia, que sigue siendo el único fin de su conservación, y en todo caso al final de la emergencia sanitaria. Los ciudadanos deben tener la certeza de que se garantiza el respeto de los derechos fundamentales y de que la aplicación se utilizará solo para fines específicamente definidos, que no se utilizará para la vigilancia masiva y que la gente seguirá teniendo el control de sus propios datos.

El Grupo de Trabajo ISS de Bioética Covid-19 ("*Gruppo di Lavoro ISS Bioetica COVID-19*") indica que el consentimiento para cualquier uso posterior de los datos con fines de investigación debe ser otorgado individualmente y con conocimiento por el usuario de la aplicación, sin que se pague ningún incentivo al usuario, directa o indirectamente[722]. Por tanto, aunque la aplicación no se creó con fines de investigación, una vez recopilados los datos se contempla la posibilidad de realizar un uso posterior de los mismos con fines de investigación. No obstante, este uso posterior deberá ser consentido por cada usuario.

6. EL TRATAMIENTO DE LOS DATOS RELATIVOS A LA SALUD CON FINES DE INVESTIGACIÓN EN IRLANDA:

En la línea de lo efectuado en el apartado anterior relativo al ordenamiento italiano, en el presente epígrafe se analizará el caso irlandés. Para ello, se estudiará la normativa aplicable, la figura del consentimiento explícito como base legitimadora para la investigación en salud, la excepción del requisito de solicitar el consentimiento explicito, cómo se ha de interpretar la figura del consentimiento amplio en la normativa irlandesa, y cómo se ha realizado el tratamiento de los datos relativos a la salud con fines de investigación en salud durante la pandemia.

6.1. Normativa aplicable:

Antes de la entrada en vigor del RGPD, en Irlanda se aplicaba la Ley de Protección de Datos número 6 de 10 de abril de 2003 *"Data Protection (Amendment) Act 2003"*. Esta

[722] GRUPPO DI LAVORO ISS BIOETICA COVID-19. Supporto digitale al tracciamento dei contatti (contact traicing) in pandemia: considerazioni di ética e di governance, (Rapporto ISS COVID-19 n.59/2020), 17 de septiembre de 2020, p. 12

ley fue adoptada para dar efecto a la Directiva 95/46/CE y enmendar la anterior Ley de Protección de Datos número 25 de 13 de julio de 1988 "*Data Protection Act 1988"*.

Con el objetivo de adaptar la normativa irlandesa al RGPD, se creó la Ley de Protección de Datos "*Data Protection Act 2018*" o "DPA" que entró en vigor el 25 de mayo de 2018. La DPA introdujo en su sección 42 disposiciones para el procesamiento de datos personales y en la sección 54 para las categorías especiales de datos personales con fines de archivo, investigación científica, histórica y estadística[723].

La particularidad de la normativa irlandesa es que, el Ministro de Sanidad, en ejercicio de las facultades conferidas por la sección 36.2 de la DPA, y habiendo cumplido debidamente los punto 5.b) y 6 de la sección 36 de la misma normativa, creó el reglamento irlandés para el procesamiento de datos personales con fines de investigación sanitaria "*S.I. No. 18/2018 - Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018*", comúnmente conocido como "HRR" por sus siglas en inglés, el cual entró en vigor el 8 de agosto de 2018. Por tanto, Irlanda cuenta con una normativa específica en el presente campo, diferenciándose de las normativas anteriormente analizadas.

Con la entrada en vigor de la HRR, se introdujeron nuevos puntos importantes para el procesamiento de datos relativos a la salud con fines de investigación sanitaria[724]. Por una parte, en el punto 1 del apartado 3 o "Regulación" tal y como lo nombra el HRR, se identifican las medidas idóneas y específicas que se han de adoptar para realizar cualquier tratamiento de datos personales con fines de investigación en salud. Es decir, a diferencia del RGPD que es técnicamente neutro como bien se ha indicado anteriormente en el apartado 2.1.3 del presente trabajo, la HRR realiza un listado de las medidas que considera idóneas y especificas para el citado procesamiento de datos personales.

En primer lugar, deben establecer disposiciones para garantizar que los datos personales se procesen "según sea necesario para lograr el objetivo de la investigación sanitaria" y no en la forma que cause o pueda causar un efecto negativo al interesado[725].

En segundo lugar, deben existir estructuras de gobernanza adecuadas. Esto incluye: la aprobación ética de la investigación por un Comité de Ética de Ínvestigación; la identificación del responsable del tratamiento; la especificación de cualquier persona que proporcione fondos para el proyecto de investigación o que lo apoye de otro modo;

---

[723] DAVIS, R., "What do Health Research Regulations 2018 mean for health researchers?", *Health Research Board*, 19 de octubre de 2018, disponible en: https://www.hrb.ie/fileadmin/1._Non-plugin_related_files/RSF_files/GDPR_guidance_for_researchers/What_do_Health_Research_Regulations_2018_mean_for_health_researchers_-_Ruth_Davies.pdf *[Última consulta: 30 de enero de 2022]*

[724] CLARKE, N.; VALE, G.; REEVES, E. P.; KIRWAN, M.; FARRELL, M.; HURL, G. y MCELVANEY, N.G., "GDPR: an impediment to research?", *Irish Journal of Medical Science (1971-)*, Vol. 188, Núm. 4, 2019, p. 1135; DAVEY, M. G.; O'DONNELL, J.P.M.; MAHER, E.; MCMENAMIN, C.; MCANENA, P.F.; KERIN, M. J.; MILLER, N.; Y LOVERY, A. J., "General data protection regulations (2018) and clinical research: perspectives of patients and doctors in an Irish university teaching hospital", *Irish Journal of Medical Science (1971-)*, Vol. 191, Núm. 4, 2021, p. 1131

[725] DONNELLY, M. y MCDONAGH, M., "Health research, consent and the GDPR exemption", *European journal of health law*, Vol. 26, Núm.2, 2019, p.112

especificación de cualquier persona que no sea responsable del tratamiento y se pretenda compartir cualquiera de los datos recopilados (incluso cuando estos datos han sido anonimizados/seudonimizados); y, la instrucción o preparación para las personas involucradas en la realización de la investigación en salud.

En tercer lugar, se requiere una evaluación del efecto que puede tener la investigación desde la perspectiva de protección de datos y, cuando esto indique un alto riesgo para los derechos y libertades de los interesados, debe llevarse a cabo una evaluación de impacto de la protección de datos (DPIA)[726]. También deben implementarse medidas que demuestren el cumplimiento del principio de minimización de datos, así como medidas para limitar el acceso a los datos personales objeto de tratamiento que eviten la consulta, alteración, divulgación o borrado no autorizados de datos personales; controles para registrar si los datos personales han sido consultado, alterado, divulgado o borrado; medidas para proteger la seguridad de los datos personales en cuestión. También deben existir medidas técnicas y organizativas diseñadas para garantizar que el procesamiento se lleve a cabo de acuerdo con el RGPD, así como procesos para probar y evaluar la efectividad de estas medidas[727].

En cuarto lugar, se deben introducir medidas para garantizar que los datos personales se procesen de manera transparente. Por último, existe el requisito de que se haya obtenido el consentimiento explícito del interesado (a menos de que sea aplicable la excepción) antes del comienzo de la investigación sanitaria, esta base legitimadora será analizada en profundidad en el siguiente apartado.

A su vez, la HRR introdujo en la Regulación 3.2 la definición del concepto de "investigación sanitaria", diferenciándose nuevamente del RGPD. Se considerará investigación sanitaria la investigación que se realice con el objetivo de comprender el funcionamiento normal y anormal, a nivel molecular, celular, de órganos y de todo el cuerpo; la investigación que se ocupa específicamente de estrategias, dispositivos, productos o servicios innovadores para el diagnóstico, tratamiento o prevención de enfermedades o lesiones humanas; la investigación que se lleve a cabo con el objetivo de mejorar el diagnóstico y el tratamiento (incluida la rehabilitación y paliación) de enfermedades y lesiones humanas y de mejorar la salud y la calidad de vida de las personas; la investigación que se efectúe con el objetivo de mejorar eficacia de los profesionales sanitarios y del sistema sanitario; y la investigación que se realice con el objetivo de mejorar la salud de la población a través de una mejor comprensión de las formas en que los factores sociales, culturales, ambientales, ocupacionales y económicos determinan el estado de salud.

---

[726] En este sentido, la universidad DCU ha creado un modelo o plantilla para realizar una Evaluación de Impacto en la Protección de Datos Personales (DPIA) para la investigación sanitaria. Véase: DCU., "Data Protection Impact Assessment", *dcu*, disponible en: https://www.dcu.ie/search-results?cx=017566043542663844620%3Ag9uk5n1hgmy&cof=FORID%3A11&keywords=Project+Screening+Questionnaire+Introduction&x=0&y=0 *[Última consulta: 2 de febrero de 2022]*

[727] DONNELLY, M. y MCDONAGH, M., "Health research, consent and the GDPR exemption", *cit.*, pp. 112-113

Así, el concepto en cuestión abarca: la investigación experimental, traslacional ("*translational*")[728] y clínica; la investigación en salud pública y atención social; la investigación en salud de la población; la investigación básica y traslacional en salud; y la investigación de estrategias de tratamiento, dispositivos médicos o desarrollo de productos. Por el contrario, la práctica habitual médica, relativa a la asistencia sanitaria, no se considera investigación científica[729]. Aunque en el citado listado no se recoge directamente a la investigación privada, debemos comprender que este ámbito se encuentra dentro del concepto de la investigación científica.

La tercera novedad introducida en la Regulación 5, es la posibilidad de solicitar una "declaración de consentimiento" para realizar nuevas investigaciones sin la necesidad de recabar el consentimiento explicito del interesado. Este concepto de "declaración de consentimiento" será desarrollado detalladamente en el apartado 5.2.2. En la misma línea, en la Regulación 6, se introduce un régimen transitorio para el otorgamiento de declaraciones de consentimiento de las investigaciones en salud ya en curso. Por último, se introdujo un Comité, "Health Research Consent Declaration Committee" o HRCDC, para la toma de decisiones sobre solicitudes de declaraciones de consentimiento, y la inclusión de un proceso de apelación[730].

6.2. El consentimiento explícito como base legitimadora para la investigación en salud:

Como se adelantaba en el aparatado anterior, la HRR identifica en su Regulación 3.1.e) al consentimiento explicito de interesado como la única base legitimadora para el procesamiento de datos personales con fines de investigación sanitaria[731]. Esto es, en Irlanda se exige un consentimiento explícito como requisito para la investigación primaria y secundaria[732]. Este consentimiento explicito debe ser otorgado antes del inicio de la investigación.

Curiosamente, a los efectos de la HRRs, el "consentimiento explícito" se define como el consentimiento obtenido de conformidad con el artículo 4 del RGPD. Esto es anómalo, ya que el artículo 4 del RGPD establece la definición de consentimiento "ordinario" en

[728] Véase al respecto: TROCHIM, W.; KANE, C.; GRAHAM, M.J. y PINCUS, H.A., "Evaluating translational research: a process marker model", *Clinical and translational science*, Vol. 4, Núm. 3, 2011
[729] DAVIS, R., "What do Health Research Regulations 2018 mean for health researchers?", *cit.*
[730] Regulaciónes 7-13 de la HRR
[731] En este sentido la Universidad Trinity College creó un modelo que recoge separadamente el consentimiento informado y el consentimiento explicito, poniendo de manifiesto la importancia de separa los respectivos consentimientos en el ámbito sanitario. TRINITY COLLEGE DUBLIN., "Guidance on the Assessment of explicit consent for health research", *tcd*, 2019, disponible en: https://nursing-midwifery.tcd.ie/research/assets/pdf/consent-form.pdf
[732] HANSEN, J.; WILSON, P.; VERHOEVEN, E.; KRONEMAN, M.; KIRWAN, M.; VERHEIJ, R. y VAN VEEN, E. B., *Assessment of the EU Member States' rules on health data in the light of GDPR*, *cit.*, 77

lugar del consentimiento explícito necesario para el tratamiento de los datos relativos a la salud que se recoge en el artículo 9.2. a) del RGPD[733].

La introducción del consentimiento explicito como única base legitimadora para el procesamiento de datos personales con fines de investigación sanitaria alarmó a los investigadores, puesto que lo concibieron como una barrera u obstáculo para el ejercicio de la investigación científica.

Se ha alegado que el Departamento de Salud adoptó un enfoque único y restrictivo para la protección de datos en Irlanda que difiere bastante de otros ordenamientos europeos, y que esto provocará un impacto negativo en la investigación clínica en Irlanda[734]. En la reunión de 25 de noviembre de 2019 organizada por la Academia Irlandesa de Ciencias Médicas se expresó que el consentimiento de los participantes ha existido durante mucho tiempo como requisito ético y legal para la realización de investigaciones sanitarias en Irlanda. Por lo tanto, el concepto de consentimiento explícito, tal como lo exige la HRR, puede parecer razonable. Sin embargo, como instrumento legal, el requisito del consentimiento explícito del participante no fomenta ni facilita la investigación en salud[735].

En este mismo sentido, GIANPERO CAVELLERI, dijo que la normativa irlandesa está fuertemente inclinada hacia el derecho a la protección de datos de los pacientes, lo cual limita la capacidad de mejorar la salud pública[736]. El mensaje político subyacente es que el consentimiento explicito es siempre la mejor opción. Según se indica, la excepción del consentimiento explicito, excepción que se analizará más adelante en profundidad, va más allá de lo requerido por el RGPD. Así, se alega que estos requisitos tendrán un efecto paralizador en la investigación en salud en Irlanda[737].

---

[733] MCCANNFITZGERALD., "New Data Protection Regulations for Health Research", *Mccannfitzgerald*, 30 de agosto de 2018, disponible en: https://www.mccannfitzgerald.com/knowledge/gdpr/new-data-protection-regulations-for-health-research *[Última consulta: 5 de febrero de 2022]*

[734] En este sentido: CLARKE, N.; VALE, G.; REEVES, E. P.; KIRWAN, M.; FARRELL, M.; HURL, G. y MCELVANEY, N.G., "GDPR: an impediment to research?", *cit.*, p. 1135; DAVEY, M. G.; O'DONNELL, J.P.M.; MAHER, E.; MCMENAMIN, C.; MCANENA, P.F.; KERIN, M. J.; MILLER, N.; Y LOVERY, A. J., "General data protection regulations (2018) and clinical research: perspectives of patients and doctors in an Irish university teaching hospital", *cit.*, p. 6

[735] MEE, B.; KIRWAN, M.; CLARKE, N.; TANAKA, A.; MANALOTO, L.; HALPIN, E.; GIBBONS,U.; CULLEN, A.; MCGARRIGLE, S.; CONNOLLY, E.; BENNETT, K.; GAFFNEY, E.; TIER, L.; FLAVIN, R. y MCELVANEY, N.G., "What GDPR and the Health Research Regulations (HRRs) mean for Ireland: a research perspective", *Irish Journal of Medical Science (1971-)*, Vol. *190*, Núm.2, 2020, p.507

[736] IRISH MEDICAL TIMES., "Data protection impact on health research assessed", imt, 11 de enero de 2019, disponible en: https://www.imt.ie/clinical/data-protection-impact-health-research-assessed-17-01-2019/ *[Última consulta: 7 de febrero de 2022]*

[737] [737] DONNELLY, M. y MCDONAGH, M., "Health research, consent and the GDPR exemption", *cit.*,117-118

En un estudio realizado en el año 2019 con Médicos de Hospital no Consultores (NCHD)[738] para determinar el conocimiento de la HRR y su percepción de la misma, el 86% indicó que la capacitación en esta nueva normativa sería útil; sin embargo, solo el 25% había recibido una formación relativa a la reforma. El 82% de los encuestados indicó que la HRR creará nuevas barreras y desafíos a la hora de llevar a cabo los proyecto de investigación, y solo el 23 % consideró que los pacientes se beneficiarán de una mayor protección de sus datos personales. Según este estudio, casi la mitad de los encuestados consideraría viajar al extranjero en busca de oportunidades de investigación[739].

Por el contrario, se ha reivindicado la importancia del consentimiento explicito en la investigación sanitaria, por empoderar al interesado, generar confianza en el mismo y conseguir que la sociedad confíe en la investigación sanitaria[740]. Se afirma que se trata de empoderar a los interesados, creando una verdadera colaboración entre los investigadores y los interesados[741]. En este sentido, en un estudio realizado en un hospital universitario irlandés en el año 2021, el 80% de los encuestados consideró que la base legitimadora del consentimiento explicito es adecuada, y reiteraron los aspectos positivos de la estricta implementación del RGPD[742].

6.3. La excepción del requisito de solicitar el consentimiento explicito:

Sin perjuicio de lo anterior, la normativa introdujo por primera vez un mecanismo lícito que permite, en circunstancias excepcionales, el tratamiento de datos personales con fines de investigación sanitaria sin el consentimiento explícito del interesado[743], debiendo realizar una aplicación o solicitud al Comité de Declaración de Consentimiento de Investigación en Salud (HRCDC por sus siglas en ingles o

---

[738] Médico de hospital no consultor ("NCHD" por sus siglas en inglés), comúnmente conocido como "médico junior", es un término utilizado en Irlanda para describir a los médicos calificados que trabajan bajo la supervisión (directa o nominal) de un consultor en una especialidad particular. Véase al respecto: NCHD., "What does that mean?", *Irish Medical Times*, 10 de mayo de 2017, disponible en: https://www.imt.ie/opinion/letters/nchd-what-does-that-mean-10-05-2017/ *[Última consulta: 12 de febrero de 2022]*

[739] WALLACE, R. y GREENE, E., "Survey of NCHDs in Ireland to assess their views and opinions in relation to participation in health research and the impact of new Irish data protection regulations", *Irish Journal of Medical Science*, Vol. 189, Núm. 3, 2020, pp. 785-787

[740] LENNON, P., "Examining the concept of consent from a legal perspective in health research", *tcd*, 28 de abril de 2021, p. 4., disponible en: https://www.tcd.ie/dataprotection/healthresearch/ *[Última consulta: 14 de febrero de 2022]*

[741] QUIGLEY, E.; HOLME, I.; DOYLE, D. M.; HO, A. K.; AMBROSE, E.; KIRKWOOD, K. y DOYLE, G., "Data is the new oil: citizen science and informed consent in an era of researchers handling of an economically valuable resource", *Life Sciences, Society and Policy*, Vol. 17, Núm. 1, 2021, pp. 11-12

[742] DAVEY, M. G.; O'DONNELL, J.P.M.; MAHER, E.; MCMENAMIN, C.; MCANENA, P.F.; KERIN, M. J.; MILLER, N.; Y LOVERY, A. J., "General data protection regulations (2018) and clinical research: perspectives of patients and doctors in an Irish university teaching hospital", *cit.*, p. 5

[743] HEALTH RESEARCH BOARD., "Health Research Regulations 2018 FAQ", *hrb*, disponible en: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/health-research-regulations-2018/health-research-regulations-2018-faq/ *[Última consulta: 15 de febrero de 2022]*

Comité)[744], quien deberá otorgar una "declaración de consentimiento" que permita dicho tratamiento. Aunque este último concepto puede llevar a confusión, podría definirse como la autorización que otorga el HRCDC para que un tratamiento de datos personales con fines de investigación sanitaria se realice sin el consentimiento explícito del interesado. Esto es, la HRCDC consiente/permite que este tratamiento pueda realizarse sin el consentimiento explícito del interesado.

Un responsable del tratamiento puede solicitar al Comité una declaración que exprese que no se requiere el consentimiento explícito del interesado, cuando el interés público de realizar la investigación en salud supere significativamente el interés público de obtener el consentimiento explícito del interesado. En consecuencia, para poder limitar el consentimiento del interesado, debe existir un interés público sólido[745]. La declaración de consentimiento es la primera alternativa legal al consentimiento que existe en Irlanda. La HRR no recoge otras alternativas al consentimiento explicito en la investigación en salud.

Para conseguir dicha declaración, el responsable del tratamiento debe realizar una "aplicación" en base a lo dispuesto en la Regulación 5 de la HRR[746]. Así, el solicitante deberá realizar una evaluación de impacto de la protección de datos de conformidad con el artículo 35.1 del RGPD; obtener la aprobación ética de la investigación en salud del Comité de Ética de la Investigación y presentar una solicitud por escrito al HRCDC que demuestre que el interés público en realizar la investigación en salud supera significativamente el interés público en requerir el consentimiento explícito del interesado[747].

El HRCDC es una entidad independiente del Comité de Ética, cuya función es revisar las aplicaciones de los investigadores[748]. El Comité debe estar compuesto por entre 15 y 21 miembros, entre los cuales deben incluirse: un presidente y un vicepresidente; personas con conocimiento de la ley de protección de datos, ética de la investigación, estadísticas u otros conocimientos relevantes y personas con experiencia en atención médica o investigación en salud[749].

---

[744] HRCDC., "About us", *hrcdc*, disponible en: https://hrcdc.ie/about-us/ *[Última consulta: 18 de febrero de 2022]*

[745] O´CONNOR, M., "Health Research Regulations 2018: Context and purpose", *hrb*, 19 de octubre de 2018, p.5, disponible en: https://www.hrb.ie/fileadmin/1._Non-plugin_related_files/RSF_files/GDPR_guidance_for_researchers/Health_Research_Regulations_2018_-_Context_and_purpose_-_Muiris_O__Connor.pdf

[746] El Comité realizó un diagrama de árbol que recoge el proceso de declaración de consentimiento de una forma clara y concisa. HRCDC,. "Decision tree: Can I apply for a consent declaration?", *hrcdc*, disponible en: https://hrcdc.ie/wp-content/uploads/2019/01/Decision_Tree_30072018.pdf

[747] SHMERLING MAGAZANIK, L., "Using Health Data for Research: Evolving National Policies", *techpolicy*, 2021, pp. 59-60, disponible en: https://techpolicy.org.il/wp-content/uploads/2021/02/Using-Health-Data-for-Research-Evolving-National-Policies-FV-.pdf

[748] HRCDC., "Overview", *hrcdc*, disponible en: https://hrcdc.ie/about-us/#Overview *[Última consulta: 20 de febrero de 2022]*

[749] HRB., "Assessment of applications for consent declarations", *hrb*, disponible en: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/consent/health-research-consent-declaration-committee/ *[Última consulta: 21 de febrero de 2022]*

Una Secretaría ubicada dentro del "*Health Research Board (HRB)*" o "Junta de Investigación en Salud", administra el proceso de Declaración de Consentimiento, y es responsabilidad de esta Secretaría velar por la eficacia del proceso. La Secretaría apoya al Comité en todos los aspectos de su trabajo y actúa como punto central de contacto para la comunidad investigadora. La Secretaría tiene una relación muy estrecha con el Departamento de Salud y la Comisión de Protección de Datos[750], los cuales han proporcionado claridad y asesoramiento muy necesarios con respecto a los asuntos de protección de datos y las Regulaciones. Gran parte de esta claridad y orientación tan necesarias se proporciona en la página web del HRCDC como un recurso para los investigadores. La Secretaría actúa como conducto entre los solicitantes y el Comité, con el objetivo de que la solicitud de una declaración de consentimiento sea un proceso sencillo. Entre las funciones claves de la secretaría destacan: la labor de apoyo al Comité, la gestión de los procesos de declaración de consentimiento y ser el punto central de contacto entre los responsables del tratamiento y el Comité[751].

Las solicitudes de declaración de consentimiento son evaluadas por un mínimo de siete miembros del Comité, de los cuales al menos uno será el presidente o vicepresidente. Una vez analizada la aplicación del responsable del tratamiento, el Comité tiene seis distintas opciones[752]: hacer una declaración de consentimiento, hacer una declaración de consentimiento sujeta a condiciones para proteger los intereses de un individuo que pueda verse afectado por la declaración de consentimiento, negarse a hacer una declaración de consentimiento, revocar una declaración de consentimiento, solicitar información adicional o consultar con cualquier persona que crea que puede asistirlo en sus deliberaciones.

Antes de otorgar una declaración, el HRCDC debe considerar que se han cumplido los requisitos establecidos en la HRR y que el interés público en llevar a cabo la investigación supera significativamente el interés público en requerir el consentimiento explícito del interesado. El Comité puede introducir ciertas condiciones que considere necesarias para proteger los intereses del interesado que puedan verse afectados por la declaración. En cuanto a la quinta opción, el Comité podrá solicitar información adicional al responsable del tratamiento. Esta información deberá ser proporcionada por el solicitante dentro de los 15 días hábiles siguientes a la realización de la solicitud o la solicitud será denegada[753].

---

[750] La Comisión de Protección de Datos (DPC por sus siglas en inglés) es la autoridad supervisora irlandesa del RGPD. Es decir, es la autoridad nacional independiente responsable de defender el derecho fundamental a la protección de datos personales a través de la aplicación y seguimiento del cumplimiento de la legislación de protección de datos en Irlanda. Fue establecida en 1989. Véase: DPC., "The Data Protection Commission", *dataprotection*, disponible en: https://www.dataprotection.ie/ *[Última consulta: 23 de febrero de 2022]*

[751] DAVIS, R., "What do Health Research Regulations 2018 mean for health researchers?", *cit.*, p. 23

[752] Ibid., p.21

[753] HRCDC., "guidance", *hrcdc*, disponible en: https://hrcdc.ie/guidance/ *[Última consulta: 23 de febrero de 2022]*

Si el Comité otorga una declaración de consentimiento, el investigador debe confirmar por escrito su aceptación dentro de los 30 días hábiles siguientes a la fecha de la notificación. Cuando el Comité no reciba dicha confirmación dentro de ese período la declaración de consentimiento caducará[754]. El Comité puede revocar una decisión cuando se da cuenta de que no se están cumpliendo las condiciones impuestas por él[755].

Cuando el Comité se niega a otorgar una declaración, adjunta condiciones a una declaración o revoca una declaración por incumplimiento de cualquier condición, el solicitante puede apelar la decisión ante el Ministro de Salud, siempre que notifique su intención de apelar dentro de los 30 días hábiles a partir de la recepción de la decisión del Comité. El Ministro debe establecer un panel de apelación independiente dentro de los 40 días hábiles para que la apelación pueda ser escuchada. Ningún miembro del Comité de Declaración de Consentimiento de Investigación en Salud formará parte de un panel de apelaciones[756].

En total, el proceso de solicitud de consentimiento que se realiza mediante la aplicación puede llegar a tener siete fases: presentación, cribado, preguntas de la secretaría, respuesta del solicitante, reunión del HRCDC, decisión, aceptación del solicitante o apelación. Desde la presentación de la aplicación hasta que el Comité responda pueden pasar entre cinco o seis semanas[757].

La HRR establece una distinción entre investigación en curso que recibió la aprobación del Comité de Ética de la investigación antes de la fecha de la entrada en vigor de la nueva normativa (8 de agosto de 2018) y la investigación aprobada después de esta fecha. En el caso de estas últimas investigaciones, tal y como se ha expuesto, se requiere el consentimiento explicito del interesado. No obstante, para el caso de las investigaciones previas a la entrada en vigor de la nueva ley, se introdujo un periodo de transición legislativa (hasta el 30 de abril de 2019) para obtener el consentimiento explícito, y cuando esto no fuese posible o los intentos fuesen infructuosos, se incluyo la posibilidad de solicitar al Comité una declaración de consentimiento[758].

Para poder realizar la aplicación, se identifican dos distintas situaciones. La primera se refiere a la existencia de un interés público significativo que deberá ser analizado por el Comité. En cuanto al segundo escenario, recoge el caso en el cual el responsable del tratamiento obtuvo el consentimiento del interesado para el tratamiento de sus datos en base a las Leyes de Protección de Datos de 1988 y 2003 (DPA 1988 y 2003) y este

[754] Regulación 9 del HRR
[755] Regulación 10.1 del HRR
[756] SHMERLING MAGAZANIK, L., "Using Health Data for Research: Evolving National Policies", *techpolicy*, *cit.*, 60
[757] Así lo indicó VEREKER, Programme Manager de la secretaría de HRCDC, en el masterclass de 28 de abril de 2021 que llevó a cabo en Trinity College. VEREKER, E., "HRCDC", *tcd*, 28 de abril de 2021, disponible en: https://www.tcd.ie/tcaid/research/healthresearchregulations.php *[Última consulta: 25 de febrero de 2022]*
[758] CLARKE, N.; VALE, G.; REEVES, E.P; KIRWAN, M.; FARRELL, M.; HURL, G. y MCELVANEY, N. G., "GDPR: an impediment to research?", *Irish Journal of Medical Science (1971-)*, Vol. 188, Núm. 4, 2019, p. 1132

consentimiento no ha sido retirado. Los requisitos que se recogen en la Regulación 6 son los mismos que se recojen en la Regulación 5, aplicable a las solicitudes posteriores al 8 de agosto de 2018. No obstante, se identifica una diferencia: si el responsable del tratamiento presenta la solicitud sobre la base de haber obtenido el consentimiento del interesado en virtud de la DPA de 1988 y 2003, debe demostrar que ha hecho todo lo posible para contactar con el interesado con el fin de volver a obtener el consentimiento del interesado[759].

6.4. El consentimiento amplio en la normativa irlandesa:

Si bien el consentimiento explícito es un requisito obligatorio para el tratamiento de datos con fines de investigación en salud, la HRR también admite el hecho de que puede ser difícil especificar completamente los propósitos de la investigación desde el principio[760]. Por ello, la normativa establece en su Regulación 3.1.e) que se puede obtener el consentimiento del interesado:

> *"explicit consent has been obtained from the data subject, prior to the commencement of the health research, for the purpose of specified health research, either in relation to a particular area or more generally in that area or a related area of health research, or part thereof."*[761]

El problema surge a la hora de interpretar esta afirmación, dado que su redacción es muy confusa y no se ha realizado ninguna guía a nivel estatal que permita a los responsables del tratamiento hacer una lectura correcta de la misma. Como bien se ha indicado anteriomente, el "consentimiento amplio" o "*broad consent*" se recoge en el Considerando 33 y artículo 7 del RGPD. En el caso de la normativa irlandesa, el HRB indica que este concepto se menciona indirectamente en la Regulación 3.1.e)[762]. El consentimiento debe ser lo más específico posible, puede ser amplio pero no general[763]. Por ende, ha de analizarse qué cubre el consentimiento amplio irlandés o, dicho de otra manera, de qué manera y en qué escala puede hacerse uso de esta herramienta.

---

[759] Regulación 6.7 de la HRR

[760] HRB., "Broad consent and the Health Research Regulations 2018", *hrb*, disponible en: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/consent/broad-consent/ *[Última consulta: 25 de febrero de 2022]*

[761] Lo cual podría traducirse como: "*se ha obtenido el consentimiento explícito del interesado, antes del comienzo de la investigación en salud, para una* ***investigación sanitaria especifica****, ya sea en relación con un* ***área en particular*** *o, de manera más general,* ***en esa área*** *o en un* ***área relacionada de investigación sanitaria****, o* ***parte de ella****.*"

[762] Esta afirmación es igualmente recogida en la guía sobre el consentimiento obtenido en el momento de la Directiva de la UE, enmienda al Reglamento de Investigación en Salud. Véase: DEPARTMENT OF HEALTH; HEALTH SERVICES EXECUTIVE; HRB Y SECRETARIAT TO HEALTH RESEARCH CONSENT DECLARATION COMMITTE., "Guidance on informed Consent obtained in the time of EU Directive Amendment to the Health Research Regulations", 2021, *hseresearch*, p. 12, disponible en: https://hseresearch.ie/data-protection-and-research/ *[Última consulta: 27 de febrero de 2022]*

[763] LENNON, P., "Examining the concept of consent from a legal perspective in health research", *cit.*, p. 3

El HRB afirma que, si el investigador no puede especificar completamente todos los fines de un proyecto en particular, el interesado puede otorgar su consentimiento para ciertas áreas de investigación sanitaria o partes de un particular proyecto de investigación[764].

En otras palabras, si dentro de un proyecto de investigación se identifican dos áreas de investigación, como pueden ser las enfermedades infecciosas y las enfermedades renales, y el investigador no puede especificar completamente todos los fines del proyecto en cuestión, se prevé la posibilidad de que el interesado otorgue el consentimiento solo para una de estas áreas, eligiendo por ejemplo las enfermedades renales. Este consentimiento será identificado como "amplio", pero será relativo a un proyecto de investigación particular. A su vez, si este proyecto tiene distintas partes las cuales no han sido totalmente especificadas al momento de la solitud del consentimiento, el interesado puede otorgar un consentimiento amplio para las partes del proyecto que considere. Dicho de una forma visual, si el proyecto tiene tres partes (parte 1, parte 2 y parte 3), y aunque los fines de estas tres partes no estén completamente especificados, el interesado podrá otorgar un consentimiento amplio por ejemplo para la parte 1.

Se trata de dar a las personas opciones de consentimiento en cada etapa del proceso de investigación. Una persona puede dar su consentimiento para: el inmediato tratamiento de datos relativo a un estudio de investigación; para el siguiente nivel de investigación que podría contemplarse; o para el uso de sus datos para preguntas/temas de investigación más generales en el área de investigación especificada o en un área relacionada de investigación en salud, que no se puede contemplar en el momento de solicitud del consentimiento[765].

Respecto al uso futuro de los datos relativos a la salud, si en el proceso de asegurar el consentimiento amplio el investigador ha proporcionado la mayor cantidad de información posible sobre posibles tratamientos futuros (información sobre los responsables del tratamiento, mecanismos de supervisión, financiadores, almacenamiento de datos, categorías de investigadores o instituciones con las que se pueden compartir los datos, transferencias nacionales e internacionales, etc.), no será necesario volver a contactar constantemente al interesado para solicitarle su consentimiento. En caso de que no se haya podido otorgar toda esta información y el interesado haya otorgado un consentimiento amplio, una vez se haya especificado cada punto, se le volverá a solicitar el consentimiento[766.]

Esto es, si el investigador ha podido proporcionar al interesado toda esta información para el tratamiento de sus datos relativos a la salud para el siguiente nivel del proyecto de investigación en cuestión; o para resolver preguntas o cuestiones más generales de aquella que pretendía responder el proyecto inicial para el cual el interesado otorgó su

[764] HRB., "Broad consent and the Health Research Regulations 2018", *cit*.
[765] Health Research Board. Health Research Regulations 2018 faq. Disponible en: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/health-research-regulations-2018/health-research-regulations-2018-faq/ *[Última consulta: 27 de febrero de 2022]*
[766] HRB., "Health Research Regulations 2018 FAQ", *cit.*

consentimiento; o para un proyecto cuya área de investigación tenga relación directa con el área de investigación en el cual se sitúe el proyecto inicial, no será necesario solicitar nuevamente el consentimiento del interesado. En caso de que no se haya cumplido con dicho objetivo, se tendrá que solicitar posteriormente el consentimiento al interesado para los nuevos tratamientos de sus datos relativos a la salud. Dado que la información a otorgar es extensa, puede afirmarse que el consentimiento amplio irlandés tiene grandes limitaciones.

6.5. El tratamiento de los datos relativos a la salud con fines de investigación durante la pandemia:

En el ámbito de la pandemia, la base legitimadora para el tratamiento de los datos relativos a la salud con fines de investigación sanitaria ha seguido siendo el consentimiento explicito del interesado.

Sin perjuicio de lo anterior, el Ministro de Salud estableció un Comité Nacional de Ética de Investigación (NREC por sus siglas en inglés) temporal para COVID-19 para acelerar el proceso de revisión ética de todas las investigaciones relacionadas con el COVID-19. La creación del Comité se justificó en la necesidad de acelerar la aprobación ética de estudios urgentes para hacer frente a la emergencia sanitaria. Se compone de 15 miembros[767] que representan una amplia gama de conocimiento, con experiencia previa en Comités de Ética locales para garantizar los más altos estándares de revisión ética y una rápida toma de decisiones[768].

El Comité ha revisado todas las solicitudes de los estudios de investigación relacionados con el COVID-19 que se incluyen en la definición de "investigación en salud" del HRR, lo cual incluye: todos los ensayos clínicos del COVID-19, incluidos los ensayos clínicos de productos sanitarios en investigación y los ensayos con dispositivos médicos, los estudios de observación y todos los estudios de intervención del virus; estudios interinstitucionales de COVID-19; estudios del virus a nivel nacional y estudios internacionales en los que ha participado Irlanda y estudios de COVID-19 que, directa o indirectamente, dan como resultado el establecimiento o la expansión de un biobanco[769].

El NREC para COVID-19 ha trabajado en estrecha relación con el Departamento de Salud y otros organismos, incluido el HRCDC y la Autoridad Reguladora de Productos ("Products Regulatory Authority" o "HPRA")[770]. Esto significa que el proceso de revisión de ética para la investigación relacionada con COVID19 se ha ejecutado en

[767] NREC COVID-19., "Members", *nrecoffice*, disponible en: https://www.nrecoffice.ie/committees/nrec-covid-19/members/ *[Última consulta: 1 de marzo de 2022]*

[768] SHEEHY, A.; JAMES, J.R.; HORGAN, M., "Implementing a National Approach to Research Ethics Review during a Pandemic-the Irish Experience", *HRB Open Research*, 2020, p.4, doi:10.12688/hcbopenres.12146.1

[769] NREC COVID-19., "Overview", *hrb*, disponible en: https://www.hrb.ie/covid-19-ethical-review/nrec-covid-19-overview/ *[Última consulta: 1 de marzo de 2022]*

[770] HRB., "New National Research Ethics Committe for Covid-19 research", 20 de abril de 2020, *hrb*, disponible en: https://www.hrb.ie/news/covid-19-coronavirus/coronavirus-news/article/new-national-ethics-committee-for-covid-19-research/ *[Última consulta: 1 de marzo de 2022]*

paralelo y en coordinación con los procesos de declaración de consentimiento. Es decir, siguiendo la excepción recogida en la Regulación 5 del HRR, se introdujo la posibilidad de que los investigadores que quisieran realizar el tratamiento de los datos relativos a la salud para la investigación del COVID-19, pudieran realizar una aplicación que demostrase que el interés público en realizar la investigación en salud superaba significativamente el interés público en requerir el consentimiento explícito del interesado.

Para agilizar el proceso a la comunidad investigadora, los requisitos tanto para el NREC para COVID-19 como para el HRCDC se incorporaron en un solo formulario[771]. Esto es, con el fin de facilitar el proceso de presentación y evitar la duplicación, el formulario del NREC COVID-19 incorporaba secciones adicionales para cuando se requería una declaración de consentimiento del HRCDC. Esta última solicitud era direccionada a la Secretaría del HRCDC por la oficina de NREC para COVID-19. Si el ensayo clínico era relativo a un medicamento en investigación o un dispositivo médico, la solicitud también tenía que ser presentada a la Autoridad Reguladora de Productos Sanitarios ("Health Products Regulatory Authority" o "HPRA")[772].

El NREC para COVID-19 respondía en un plazo máximo de 7 días desde que se realizaba la solicitud, contestando mediante email a los solicitantes. Durante su mandato (desde el mes de abril al mes de agosto de 2020), el NREC para COVID-19 revisó 93 solicitudes[773], de las cuales cuatro fueron denegadas. El NREC COVID-19 llegó al final de su mandato, creándose un subcomité permanente del NREC COVID-19 para revisar las solicitudes de enmiendas a los estudios que recibieron la aprobación del NREC COVID-19, siendo la última fecha para la solicitud de enmienda el 31 de agosto de 2022.

A modo de ejemplo, podemos analizar dos distintas aplicaciones para la solicitud de consentimiento de dos proyectos de investigación del COVID-19, nombradas como aplicación 20-006-AF1/COV y 20-007-AF1/COV, analizadas en la reunión de 15 de abril de 2020[774], con el fin de ver cómo ha valorado en la práctica el HRCDC si el interés público de realizar la investigación en salud supera significativamente el interés público de obtener el consentimiento explícito del interesado en el ámbito de la pandemia. Esto es, este ejercicio permitirá saber cómo ha valorado el HRCDC este interés público, siendo de gran interés para el presente trabajo.

---

[771] NREC COVID-19., "Apply", hrb, disponible en: https://www.hrb.ie/covid-19-ethical-review/apply/ *[Última consulta: 1 de marzo de 2022]*

[772] HRB., "Frequently asked questions", *hrb,* disponible en: https://www.hrb.ie/funding/manage-a-grant/faq/ *[Última consulta: 2 de marzo de 2022]*

[773] En la página oficial de la NREC para COVID-19 están disponibles todas las aplicaciones que se presentaron. NREC COVID-19., "Decisions", *nrecoffice*, disponible en: https://www.nrecoffice.ie/committees/nrec-covid-19/decisions/ [Última consulta: 1 de marzo de 2022]

[774] HRCDC., "Meeting", hrcdc, 15 de abril de 2020, disponible en: https://hrcdc.ie/wp-content/uploads/2020/05/HRCDC-Meeting-Minutes-15.04.2020-APPROVED.pdf

La primera aplicación era relativa a un ensayo aleatorio doble-ciego controlado con placebo[775] de antitripsina alfa-1 (proteína que ayuda a disminuir la inflamación) purificada en plasma para hacer frente al COVID-19[776]. El objetivo de este estudio era examinar si la administración de esta proteína por vía intravenosa a pacientes con COVID-19 y Síndrome de Dificultad Respiratoria Aguda en la UCI puede ayudar a reducir la inflamación y, en consecuencia, ayudar a la recuperación de los mismos. Se solicitaba una declaración de consentimiento para tratar los datos personales de los interesados que, por encontrarse en la UCI, no tenían capacidad de otorgar su consentimiento.

Se solicitaba la declaración de consentimiento para la recogida y tratamiento de datos de la historia clínica de los interesados; el almacenamiento de los datos personales para futuras investigaciones, y el análisis de las muestras de sangre vinculadas a los datos personales. El HRCDC consideró que el estudio tenía un gran interés público, puesto que el tratamiento podría beneficiar positivamente a los pacientes con COVID-19, pero señaló que para este estudio se implementaría un modelo de consentimiento diferido, que requiere la solicitud de consentimiento al pariente más cercano del interesado, permitiendo el consentimiento telefónico o medios similares cuando no fuese posible obtener el consentimiento en persona.

En cuanto a la segunda aplicación, concernía al proyecto para la integración de análisis de datos de pacientes críticos de COVID-19. El objetivo del proyecto era analizar los datos relativos a la salud de cincuenta pacientes de COVID-19 que se encontraban en la UCI del Hospital "St James" para buscar "patrones" o correlaciones entre tratamientos y respuestas durante los cuidados intensivos. Los datos provendrían de registros electrónicos generados en el hospital durante el seguimiento continuo de los pacientes. La UCI del hospital tenía el objetivo de trabajar con un centro de investigación llamado CeADAR, especializado en análisis de datos e Inteligencia Artificial. Para ello, se pretendía enviar una gran cantidad de datos seudonimizados, fruto de la monitorización del paciente, al CeADAR para su análisis. Una vez enviados, se utilizaría un algoritmo informático para "interrogar" a los datos y buscar relaciones dentro de los datos. Se pretendía que esta correlación ayudara a la toma de decisiones médicas.

---

[775] Se refiere al ensayo clínico en el cual los participantes son separados aleatoriamente en dos grupos. Un grupo de participantes (grupo testigo) recibe un medicamento inactivo, que recibe el nombre de placebo, mientras que otro grupo de participantes (grupo experimental) recibe el medicamento activo sometido a prueba. Ni los participantes ni los investigadores sabrán a qué grupo pertenece cada participante durante el periodo que dura la experimentación. Véase al respecto: CÍNICA UNIVERSIDAD DE NAVARRA., "Diccionario médico", *cun*, disponible en: https://www.cun.es/diccionario-medico *[Última consulta: 2 de marzo de 2022]*

[776] La alfa 1 antitripsina (AAT) es una proteína natural que se encuentra en el cuerpo humano. Una de las principales funciones beneficiosas de la AAT es disminuir la inflamación. Esto es importante en el contexto de COVID-19 dado que una de las características de la enfermedad es la inflamación del pulmón. Esta inflamación puede provocar daño pulmonar, fallo multiorgánico y, en casos severos, la muerte. Una parte sustancial de los pacientes que mueren por COVID-19 lo hacen por el Síndrome de Dificultad Respiratoria Aguda (SDRA). La SDRA es esencialmente una insuficiencia pulmonar que se produce por una inflamación del pulmón que provoca una disminución de oxígeno y acumulación de líquido en el pulmón.

Se solicitaba una declaración de consentimiento para revisar las historias clínicas electrónicas de los pacientes, recopilar datos, seudonimizarlos, transferirlos al procesador de datos y aplicar la inteligencia artificial. No obstante, el HRCDC consideró que sería apropiado y factible intentar obtener el consentimiento explicito de los 50 participantes del estudio, o implementar el modelo de consentimiento diferido, requiriendo la solicitud de consentimiento al pariente más cercano del interesado.

El HRCDC señaló que el estudio tenía cierto grado de interés público al desarrollar un programa de Inteligencia Artificial que tenía el potencial de respaldar la toma de decisiones clínicas dentro de la Unidad de Cuidados Intensivos. Sin embargo, el Comité indicó que, si bien los resultados del estudio podían influir positivamente en el tratamiento clínico y el manejo de los pacientes con COVID-19, era poco probable que el uso y el impacto de los resultados se viese a corto o medio plazo. A su vez, el HRCDC no estaba convencido de que este tamaño de cohorte fuese suficiente para producir resultados que pudieran proporcionar un impacto científico significativo, o si el resultado del modelo de IA se usaría de inmediato o se confiaría en él para tratar a los pacientes. Al sopesar los citados puntos de discusión, el HRCDC declaró que el impacto científico general del estudio no era de interés y beneficio público significativo, no pudiendo limitar el consentimiento explicito del interesado.

En cuanto a la aplicación de rastreo de COVID-19, Irlanda creo la aplicación COVID Tracker. Para su creación, se siguió el modelo descentralizado[777], y fue diseñada de manera que se minimizara la cantidad de datos personales procesados para cumplir con los propósitos definidos[778]. El Servicio de Salud de Irlanda (HSE) abordó los problemas de su aplicación mediante la evaluación de impacto que puso a disposición del público[779]. En este sentido, un estudio realizado para averiguar la percepción de la aplicación de los irlandeses, indicó que aunque los usuarios apreciaban la transparencia del HSE (por ejemplo mediante actos como la publicación de la DPIA), el sentimiento

[777] Las aplicaciones de rastreo de COVID-19 han adoptado distintas arquitecturas para la recopilación de datos. Estas arquitecturas se clasifican predominantemente en dos categorías: centralizadas y descentralizadas. Dentro de la arquitectura centralizada, la mayor parte de la información se almacena y procesa en un servidor en la nube centralizado. En este enfoque, el servidor en la nube juega un papel clave al almacenar los datos seudonimizados de los usuarios, realizar análisis de riesgo y enviar notificaciones a contactos cercanos en caso de infección. Esto plantea problemas de seguridad y privacidad con respecto al uso y el ciclo de vida de los datos recopilados, especialmente si el servidor en la nube se convierte en una entidad no confiable. En una arquitectura descentralizada, las funciones principales se trasladan a los dispositivos de los usuarios, lo que reduce drásticamente la participación del servidor centralizado en el proceso de seguimiento de contactos. Este enfoque intenta mejorar el derecho a la protección de datos del usuario al realizar el proceso de rastreo localmente en el dispositivo del mismo. Las aplicaciones de seguimiento de contactos basadas en el enfoque descentralizado no requieren que los usuarios se registren previamente antes de su uso y, como consecuencia, no se almacena información de identificación personal en el servidor. Véase al respecto: TRESTIAN, R.; XIE, G.; LOHAR, P.; CELESTE, E.; JAYASEKERA, E.; CONNOLLY, R. y TAL, I., "Privacy in a Time of COVID-19: How Concerned Are You?", *IEEE Security & Privacy*, vol. 19, Núm. 5, 2021, p. 27-28

[778] HSE., "Data Protection Impact Assessment Covid Tracker App", 26 de junio de 2020, disponible en: https://www.hse.ie/eng/services/news/newsfeatures/covid19-updates/covid-tracker-app/covid-tracker-app.html *[Última consulta: 5 de marzo de 2022]*

[779] TRESTIAN, R.; XIE, G.; LOHAR, P.; CELESTE, E.; JAYASEKERA, E.; CONNOLLY, R. y TAL, I., "Privacy in a Time of COVID-19: How Concerned Are You?", *cit*., p. 28

general, era que estaban sacrificando su privacidad[780]. Sin perjuicio de lo anterior, el uso de la aplicación ha sido totalmente voluntario[781].

7. LA COMPARACIÓN DE LA REGULACIÓN ESPAÑOLA CON NORMAS FORANEAS Y LAS PROPUESTAS QUE SE DERIVAN DE ESTE EJERCICIO:

Una vez finalizado el análisis de las tres normativas seleccionadas, resulta necesario realizar una comparación de las mismas con el objetivo de resaltar las divergencias que existen entre los distintos modelos normativos, lo cual refleja la falta de armonización legislativa en este ámbito y lo exiguo del avance que ha supuesto el RGPD en materia de investigación sanitaria. Tras efectuar esta acción, se procederá a indicar las propuestas que se derivan del mismo ejercicio de llevar a cabo la comparación.

7.1. Elección del instrumento regulador:

El legislador español optó por regular el tratamiento de los datos en la investigación en salud en la Disposición Adicional Decimoséptima de la LOPGDGDD, siendo esta opción criticable dada la importancia de la investigación sanitaria. Dentro de esta Disposición Adicional se identifican cuatro bases legales, las cuales requieren un arduo ejercicio de interpretación debido a su compleja redacción.

El consentimiento del interesado recogido en el apartado 2.a) de la D.A.17ª es realmente amplio, permitiendo que el consentimiento otorgado, por ejemplo, para la investigación del cáncer de pulmón pueda ampliarse al ámbito oncológico, lo cual plantea la pregunta de si, debido a su amplitud, este consentimiento realmente respeta los principios recogidos en el RGPD. A su vez, en la normativa española existen otras tres bases legitimadoras que permiten realizar el tratamiento de los datos relativos a la salud con fines de investigación: situaciones de excepcional relevancia y gravedad para la salud pública, la reutilización de los datos personales para finalidades o áreas de investigación relacionadas con el área en la que se integrase científicamente el estudio inicial, y el uso de datos personales seudonimizados; cabiendo afirmar que el legislador ha apostado firmemente por la investigación científica.

Respecto a las medidas de seguridad, estas se regulan en las letras e), f) y g) del apartado segundo de la D.A.17º. Se deberían de haber separado de las bases legales, y no redactar las mismas en el mismo punto que las bases legales. A su vez, su redacción es muy confusa y se ha de realizar nuevamente una interpretación para saber en qué situaciones han de ser aplicadas.

En el caso de Italia, este ámbito se regula en dos artículos del Código, separando el tratamiento de los datos relativos a la salud para la investigación médica, biomédica e

[780] LOHAR, P.; XIE, G.; BENDECHACHE, M.; BRENNAN, R.; CELESTE, E.; TRESTIAN, R. y TAL, I., "Irish attitudes toward COVID tracker app & privacy: sentiment analysis on Twitter and survey data", *cit.*, p.7
[781] HSE., "Data Protection Impact Assessment Covid Tracker App", *cit.*

epidemiológica del tratamiento posterior de los datos personales con fines estadísticos o de investigación científica. Aunque el consentimiento del interesado sea la regla para el tratamiento de los datos relativos a la salud para investigación médica, biomédica e epidemiológica, se introducen dos grandes excepciones: que la investigación se lleve a cabo sobre la base de disposiciones legales o reglamentarias o del Derecho de la Unión Europea de conformidad con el artículo 9.2.j) del RGPD o cuando la investigación sea parte de un programa de investigación biomédica o sanitaria contemplado en el artículo 12 bis del Decreto legislativo 502/1992; o cuando, por motivos particulares, sea imposible o implique un esfuerzo desproporcionado informar a los interesados o se pueda imposibilitar o comprometer gravemente el logro de los fines de investigación.

Dentro de la segunda excepción, se identifican tres distintos escenarios que representan dicha imposibilidad, esfuerzo desproporcionado o riesgo: motivos éticos, razones de imposibilidad organizativa y razones de salud atribuibles a la gravedad del estado clínico del interesado. Aunque gracias a la creación de estos tres supuestos se ha tratado de clarificar la idea subyacente del artículo 110 del Código, este ámbito sigue siendo confuso. Será la practica quien nos indique en qué situaciones se admite el argumento de imposibilidad, esfuerzo desproporcionado o riesgo, para poder realizar el tratamiento de los datos relativos a la salud sin el consentimiento del interesado.

A su vez, el Garante puede autorizar el procesamiento posterior de los datos personales con fines de investigación científica a terceros que realicen principalmente estas actividades cuando, por motivos particulares es imposible informar a los interesados o es probable que haga imposible o afecte gravemente al logro de los objetivos de la investigación, siempre que se tomen medidas apropiadas para proteger los derechos, libertades e intereses del interesado. Así, aunque el legislador italiano identifique al consentimiento del interesado como la "regla" para el procesamiento de los datos relativos a la salud, posteriormente introduce multitud de excepciones. Estas excepciones también requieren un acto de interpretación, lo cual crea problemas para los investigadores.

Irlanda, por su parte, cuenta con una normativa propia para el tratamiento de datos personales con fines de investigación sanitaria, diferenciándose positivamente de los dos anteriores sistemas. En la normativa se introdujo el consentimiento explícito como la base legitimadora para el procesamiento de datos personales con fines de investigación sanitaria, siendo la declaración de consentimiento el único mecanismo lícito que permite, en circunstancias excepcionales, dicho tratamiento sin el consentimiento explícito del interesado.

Como crítica, puede alegarse que, en realidad, en el modelo irlandés existen dos bases legitimadoras: el consentimiento explícito y el interés público. Esto es, aunque mediante la redacción de la norma se ha pretendido reivindicar que en Irlanda la única forma de realizar el tratamiento datos personales con fines de investigación sanitaria sea el consentimiento explícito del interesado, mediante la incorporación de la autorización del HRCDCC como excepción a la norma, en realidad se han introducido dos bases

legitimadoras, no una. El objetivo era hacer creer a los interesados que, en todo momento, van a tener el control sobre sus datos relativos a la salud, pero de una forma un tanto enrevesada se introdujo una nueva base legal. En suma, no es cierto que en Irlanda la única base legitimadora para realizar el tratamiento de los datos relativos a la salud con fines de investigación sanitaria sea el consentimiento del interesado, también existe la base legal del interés público.

7.2. El tratamiento de los datos relativos a la salud con fines de investigación que se ha realizado en la pandemia:

La AEPD no ha publicado ninguna guía que permita saber cómo ha de interpretarse y aplicarse la D.A. 17ª de la LOPDGDD en una circunstancia tan excepcional como la provocada por el COVID-19. Aunque el consentimiento del interesado ha seguido siendo una base legitimadora más, los investigadores han podido utilizar otras vías más sencillas, lo cual les ha permitido evitar solicitar el consentimiento a los interesados en ciertas situaciones. Las autoridades sanitarias e instituciones públicas con competencias en vigilancia de la salud pública han podido llevar a cabo estudios científicos sin el consentimiento de los interesados, incluso manteniendo los datos de identificación de los mismos. A su vez, los grupos de investigación tanto públicos como privados han tenido la oportunidad de realizar un uso secundario de los datos de salud mediante la seudonimización de los mismos y la autorización del correspondiente Comité de Ética de la Investigación. Sin perjuicio de lo anterior, en España no existe un registro que permita verificar la base legitimadora que ha sido utilizada en cada proyecto.

El Garante ha adoptado una actitud proactiva introduciendo una derogación parcial del artículo 110 del Código, lo cual ha permitido a los responsables del tratamiento realizar los tratamientos de datos relativos a estudios experimentales y usos compasivos de medicamentos de uso humano para el tratamiento y prevención del virus sin la necesidad de presentar previamente el proyecto de investigación y realizar la evaluación de impacto y la consulta previa al Garante. Llama realmente la atención la permisibilidad del sistema italiano, puesto que, los investigadores han tenido la posibilidad de no presentar ni tan siquiera el proyecto de investigación, todo ello bajo el paraguas de la excepcionalidad de la situación. No obstante, esta transigencia pone directamente en peligro el derecho a la protección de datos de los interesados.

En contraste en Irlanda, en el ámbito de la pandemia, la base legitimadora ha seguido siendo el consentimiento explícito del interesado, identificando la declaración de consentimiento como la única excepción a la regla. Como novedad, se ha introducido un Comité Nacional de Ética de Investigación temporal para COVID-19 para acelerar el proceso de revisión de ética de todas las investigaciones relacionadas con la enfermedad. Por ende, Irlanda ha seguido apostando por tratar de otorgar el "control" de los datos relativos a la salud a los interesados hasta en una situación de emergencia sanitaria, aunque dicha apuesta haya conllevado mayores exigencias para los investigadores irlandeses en comparación con los anteriores modelos normativos.

En cuanto a la valoración del interés público realizada por el HRCDC en el contexto de la pandemia, en la página oficial del HRCDC están disponibles todas las aplicaciones que se han presentado y cómo se ha valorado si realmente existe este interés público o no en cada caso. De esta manera, de la lectura de todas estas aplicaciones se pueden identificar los requisitos necesarios que han tenido que cumplirse para que el HRCDC haya otorgado la declaración de consentimiento. El hecho de que todas estas reuniones de valoración de las aplicaciones estén disponibles en la página oficial del HRCDC, es un gran ejemplo de transparencia que ha de ser subrayado, España debería haber seguido el ejemplo de Irlanda.

7.3. Propuestas que se derivan de la comparación:

La siguiente tabla sintetiza lo dicho hasta el momento:

	REGULACIÓN	**BASE LEGITIMADORA**	**COVID-19**
ESPAÑA	D.A.17ª.2 de la LOPDGDD	4	La AEPD no se ha pronunciado, amplias opciones para los investigadores
ITALIA	Artículos 110 y 110 bis del Código	Consentimiento + múltiples excepciones	Derogación parcial del artículo 110 del Código
IRLANDA	Normativa específica	Consentimiento explícito + la "declaración de consentimiento" o autorización del HRCDC	Consentimiento explícito + introducción del NREC temporal para COVID-19, gran transparencia

Una vez esquematizado lo indicado anteriormente mediante la presente tabla, cabe alegar que, aunque ninguno de los tres sistemas es perfecto, puede defenderse que el modelo irlandés es más adecuado que el español o el italiano. Para empezar, a diferencia de España o Italia, en Irlanda se ha apostado acertadamente por crear una ley específica para este ámbito tan importante. Su redacción es bastante adecuada, no debiendo realizar la ardua tarea de interpretación que sí exigen los dos modelos restantes.

Sin perjuicio de lo anterior, hoy en día no es realista defender que la base legal para el tratamiento de los datos relativos a la salud con fines de investigación sanitaria tenga que ser en todo caso, y sin excepción alguna, el consentimiento explícito del interesado, puesto que no siempre es posible recabar este consentimiento, y con este requisito obligatorio se estaría restringiendo la investigación sanitaria. No obstante, como se viene reiterando, en Irlanda existe la posibilidad de realizar el tratamiento que nos

incumbe sin el consentimiento explícito del interesado cuando el interés público en llevar a cabo la investigación sea significativamente superior, siendo esta una muy buena solución para el problema expuesto. El control o análisis que hace el HRCDC es una herramienta que ampara el derecho a la protección de datos personales de los interesados. Tal y como se ha alegado en numerosas veces durante este trabajo, el valor de la investigación sanitaria es indiscutible, pero este hecho no justifica cualquier tratamiento de los datos relativos a la salud en nombre de la investigación sanitaria. No todo vale, ha de existir un equilibrio.

En este sentido, la pandemia ha remarcado la necesidad de encontrar el equilibrio entre la urgencia por alcanzar resultados que permitan combatir la pandemia, y desarrollar una investigación respetando los derechos de los interesados. Solo si se logra esa conciliación se alcanza un avance sólido en el conocimiento sin menoscabar los derechos individuales. Los derechos humanos nunca pueden desaparecer ante el interés general, el derecho a la protección de datos personales no puede liquidarse con el objetivo de acelerar el avance de la ciencia[782].

El RGPD perpetúa el enfoque fragmentado de la protección de datos personales en la investigación en salud, los estados miembros de la UE difieren en la forma en que interpretan los requisitos del reglamento[783]. El problema es que se ha dejado que los países europeos individuales decidan cómo se pueden tratar los datos relativos a la salud para la investigación en salud. Esta flexibilidad estaba destinada a permitir que los países se ajustasen a la cultura, tecnología y sistemas propios, pero ha tenido como resultado la falta de sintonía entre países. Todo esto dificulta que se lleven a cabo proyectos de investigaciones comunes entre los distintos estados miembros, puesto que, por ejemplo, la normativa de un país participante puede permitir el tratamiento posterior de los datos recopilados sin la necesidad de recabar nuevamente el consentimiento del interesado y la normativa de otro país participante no.

El RGPD corre el riesgo de convertirse en una directiva en el contexto de la investigación científica, dado que, al igual que con la derogada Directiva de protección de datos, se permite que los Estados miembros determinen las garantías nacionales apropiadas para el procesamiento de datos con fines de investigación científica[784]. Para una jurisdicción como Irlanda, que adopta un enfoque exigente y diferenciado del requisito del consentimiento explícito, la consecuencia puede ser la exclusión de los proyectos de investigación en salud a nivel europeo y una reducción general de los proyectos de investigación en salud[785]. España por su parte ha adoptado un enfoque

[782] CBE. Informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de Covid-19, *cit.*, p. 20

[783] EISS, R., "Confusion over data-privacy law stalls scientific progress", *Nature*, 25 de agosto de 2020, disponible en: https://www.nature.com/articles/d41586-020-02454-7 *[Última consulta: 10 de marzo de 2022]*

[784] DOVE, E.S., "The EU general data protection regulation: implications for international scientific research in the digital era", *Journal of Law, Medicine & Ethics*, Vol. 46, Núm. 4, 2018, pp. 1027-1028

[785] DONNELLY, M. y MCDONAGH, M., "Health research, consent and the GDPR exemption", *cit.*, p. 119

totalmente contrario, quitándole trabas a la investigación en salud, aunque, a su vez, ha vaciado de contenido el consentimiento del interesado.

Por todo lo antedicho, se precisa una reforma que armonice la investigación sanitaria. Las bases legales del RGPD han de ser claras, no confusas, e iguales para todos los países europeos. Igualmente, se ha de apostar por indicar detalladamente cuáles son las medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado, el RGPD no puede mantener una posición pasiva en este aspecto, ha de pronunciarse.

8. FORMULARIO EUROPEO DE CONSENTIMIENTO PARA LA CESIÓN ALTRUISTA DE DATOS:

8.1. Breve introducción al Reglamento de Gobernanza de Datos:

Con el fin de fomentar un uso secundario de la información del sector público para la innovación en productos y servicios, se adoptó la Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público (DDA)[786]. La Comisión consideró que era necesario actuar a escala de la Unión para afrontar los obstáculos restantes y emergentes a una amplia reutilización de la información del sector público y financiada con fondos públicos en toda la Unión y actualizar el marco legislativo con los avances en las tecnologías digitales, y estimular aún más la innovación digital, en especial en lo que respecta a inteligencia artificial. No obstante, la DDA no es aplicación a los datos personales[787].

Ante esta realidad, se creó el Reglamento 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022 relativo a la gobernanza de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos o RGD), el cual es aplicable a los datos que obren en poder de organismos del sector público que estén protegidos por motivos de confidencialidad comercial; confidencialidad estadística; protección de los derechos de propiedad intelectual de terceros, o protección de los datos personales[788]. Por tanto, el RGD sí que contempla los datos personales.

Esta norma nace del valor económico y social que ofrece el tratamiento de los datos, puesto que su uso puede dar origen a nuevos productos y servicios basados en las nuevas tecnologías, hacer la producción más eficiente y dotar de herramientas para hacer frente a los retos sociales. En el ámbito de la salud, como ya se ha expuesto, los datos contribuyen a mejorar la asistencia sanitaria, los tratamientos personalizados y la cura de las enfermedades raras o crónicas. A su vez, se calcula que el intercambio de los

[786] DOUE núm. 172, de 26 de junio de 2019
[787] Considerando 52 de la DDA
[788] Artículo 3 del RGD

datos relativos a la salud proporcionará un ahorro de aproximadamente 120.000 millones de euros al año en el sector sanitario de la UE[789].

Su principal objetivo consiste en generar confianza[790] entre los particulares y las empresas en relación con el acceso a los datos, su control, intercambio, utilización y reutilización, especialmente mediante el establecimiento de mecanismos adecuados que permitan a los interesados conocer y ejercer de forma significativa sus derechos y, en lo relativo a la reutilización de determinados tipos de datos que obren en poder de organismos del sector público, la prestación de servicios a los interesados, a los titulares de datos y a los usuarios de datos, por parte de los proveedores de servicios de intermediación de datos, así como la recogida y el tratamiento de datos cedidos con fines altruistas por personas físicas y jurídicas[791]. Esto es, el fin es promover la disponibilidad de los datos y construir un entorno confiable para facilitar su uso para la investigación y la creación de nuevos servicios y productos innovadores[792].

Dentro del RGD, se identifican tres principales subgrupos: la reutilización de determinadas categorías de datos protegidos que obren en poder de organismos del sector público[793]; los servicios de intermediación de datos[794]; y la cesión altruista de datos, la cual será objeto de análisis de los siguientes puntos debido a su relación directa con la base legal del consentimiento del interesado que constituye el núcleo del presente capítulo.

8.2. La cesión altruista de datos:

La cesión altruista de datos es definida en el artículo 2.16 del RGD como todo intercambio voluntario de datos basado en el consentimiento de los interesados para que se traten sus datos personales, o en el permiso de los titulares de datos para que se usen sus datos no personales, sin ánimo de obtener o recibir una gratificación que exceda de

[789] COMISIÓN EUROPEA., "European data governance", *digital-strategy.ec.europa.eu*, 23 de junio de 2021, disponible en: https://digital-strategy.ec.europa.eu/en/policies/data-governance [*Última consulta: 2 de noviembre de 2022*].

[790] Para aprovechar este potencial, se manifiesta que deben ponerse a disposición más datos, compartirse con confianza y hacer que sean fácilmente reutilizables desde el punto de vista técnico. Véase al respecto: RODRÍGUEZ PITA, P., "Reglamento sobre gobernanza de los datos", *economiadigital*, 5 de diciembre de 2020, disponible en: http://economiadigital.etsit.upm.es/reglamento-sobre-la-gobernanza-de-los-datos/ [*Última consulta: 2 de noviembre de 2022*].

[791] Considerando 5 del RGD

[792] ABOGACÍA ESPAÑOLA., "El Consejo de la UE aprueba el Reglamento de Gobernanza de Datos", *abogacía*, 17 de mayo de 2022, disponible en: https://www.abogacia.es/actualidad/noticias/el-consejo-de-la-ue-aprueba-el-reglamento-de-gobernanza-de-datos/ [*Última consulta: 2 de noviembre de 2022*].

[793] La reutilización es definida en el artículo 2.2 del RGD como *"la utilización, por personas físicas o jurídicas, de los datos que obren en poder de organismos del sector público, con fines comerciales o no comerciales distintos del propósito inicial englobado en la misión de servicio público para el que se hayan producido tales datos, excepto en el caso del intercambio de datos entre organismos del sector público con la única finalidad de desempeñar sus actividades de servicio público".*

[794] La intermediación de datos es definida en el artículo 2.11 del RGD como *"todo servicio cuyo objeto sea establecer relaciones comerciales para el intercambio de datos entre un número indeterminado de interesados y titulares de datos, por una parte, y usuarios de datos, por otra, a través de medios técnicos, jurídicos o de otro tipo".*

una compensación relativa a los costes en que incurran a la hora de facilitar sus datos, con objetivos de interés general tal como se disponga en el Derecho nacional, en su caso, como, por ejemplo, la asistencia sanitaria, la lucha contra el cambio climático, la mejora de la movilidad, la facilitación del desarrollo, elaboración y difusión de estadísticas oficiales, la mejora de la prestación de servicios públicos, la elaboración de políticas públicas o la investigación científica de interés general.

Podemos interpretar el altruismo como la cesión voluntaria de los datos que realizan los interesados o los titulares de datos para contribuir a la sociedad. Por tanto, la base legítima para realizar la presente cesión de los datos es el consentimiento del interesado. En el caso de que los datos sean considerados comunes, la base legitima se encontrará en el artículo 6.1.a) del RGPD, en el caso de las categorías especiales de datos personales, en el artículo 9.1.a) del RGPD[795]. El consentimiento en el que se basa la cesión altruista de datos debe reunir las características que se recogen en el RGPD para que sea considerado válido.

Aunque en el ámbito sanitario el concepto de la donación este muy presente (donación de sangre, de órganos, de tejidos…), el altruismo de datos no puede comprenderse como una donación de datos personales, puesto que ello implicaría una transferencia de propiedad sobre dichos datos personales[796]. No se trata de una transmisión de la titularidad, sino una cesión de los datos que realiza el titular de los mismos manteniendo su propiedad. Por tanto, se ha de optar por utilizar el término del altruismo de datos.

En palabras de ALKORTA IDIAKEZ este acto implica sacrificar el bienestar de uno por el bienestar de los demás sin esperar una compensación o beneficio personal. Al otorgar el consentimiento, el interesado no solo renuncia a la recompensa, sino asumir riesgos como pueden ser los problemas de seguridad en beneficio de la sociedad[797]. El altruismo de datos, o la posibilidad de poner a disposición los datos personales para la investigación, es una de las claves para el ámbito sanitario, especialmente en los Estados miembros donde prevalecen los derechos de las personas y no el interés público[798].

Los Estados podrán elaborar políticas nacionales para ayudar a los interesados a la hora de ceder voluntariamente y con fines altruistas datos personales que les conciernan y que obren en poder de organismos del sector público, al igual que podrán establecer la información necesaria que se deberá facilitar a los mismos[799].

[795] A nivel nacional, en la D.A.17ª.2.a) de la LOPDGDD
[796] HUMMEL, P; BRAUN, M y DABROCK, P., "Data Donations as Exercises of Sovereignty", En: KRUTZINA, J y FLORIDI, L., *The ethics of medical data donation*, Springer, 2019, p. 24
[797] ALKORTA IDIAKEZ, I., El espacio europeo de datos sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios, Aranzadi, Pamplona, 2022, p. 249
[798] HANSEN, J.; WILSON, P.; VERHOEVEN, E.; KRONEMAN, M.; KIRWAN, M.; VERHEIJ, R. y VAN VEEN, E. B., *Assessment of the EU Member States' rules on health data in the light of GDPR, cit.*, p. 113
[799] Considerando 47 y artículo 16 del RGA

Las organizaciones que traten de recopilar datos con fines de interés general en base a la cesión altruista de datos pueden solicitar su inscripción en un registro nacional de organizaciones reconocidas de gestión de datos con fines altruistas, lo cual genera la confianza necesaria en la cesión altruista de datos. Para que una organización pueda inscribirse en el registro de organizaciones reconocidas de gestión de datos con fines altruistas, y así considerarse una organización de gestión de datos con fines altruistas, deberá ejercer actividades de cesión altruista de datos; ser una entidad jurídica constituida con arreglo al Derecho nacional para cumplir objetivos de interés general; ejercer su actividad sin ánimo de lucro y ser independiente de cualquier entidad que ejerza su actividad con fines lucrativos; y desempeñar las actividades de cesión altruista de datos mediante una estructura jurídicamente independiente, separada de otras actividades que lleve a cabo y cumplir el código normativo[800]. Toda entidad que cumpla los citados requisitos podrá solicitar su inscripción en el registro público nacional de organizaciones reconocidas de gestión de datos con fines altruistas en el Estado miembro en el que esté establecida[801].

Cada autoridad competente para la inscripción en el registro de las organizaciones de gestión de datos con fines altruistas[802] llevará y actualizará periódicamente un registro público nacional de organizaciones reconocidas de gestión de datos con fines altruistas. Corresponderá a la Comisión llevar un registro público de la Unión de organizaciones reconocidas de gestión de datos con fines altruistas a efectos informativos. Para que dichas organizaciones sean fácilmente identificables, la Comisión creará un logotipo común que irá acompañado de un código QR con un enlace al registro público de la Unión [803].

8.3. El formulario:

Con el fin de que la recogida de los datos cedidos con fines altruistas sea más fácil, la Comisión adoptará actos de ejecución en los que se establezca y elabore un formulario europeo de consentimiento para tal cesión, previa consulta al Comité Europeo de Protección de Datos, teniendo en cuenta el asesoramiento del Comité Europeo de Innovación en materia de Datos y contando debidamente con la participación de las partes interesadas pertinentes. El formulario europeo de consentimiento para la cesión altruista de datos, en adelante "el formulario", permitirá recabar el consentimiento o el permiso en todos los Estados miembros en un formato uniforme. El formulario permitirá a los interesados otorgar o retirar su consentimiento respecto de un tratamiento

[800] Artículo 18 del RGA
[801] Artículo 19 del RGA
[802] En base al Considerando 51: *"las autoridades competentes para la inscripción en el registro de las organizaciones de gestión de datos con fines altruistas designadas para supervisar el cumplimiento de los requisitos del RGA por las organizaciones reconocidas de gestión de datos con fines altruistas han de ser elegidas en función de su capacidad y conocimientos especializados. Deben ser independientes de cualquier organización de gestión de datos con fines altruistas, así como transparentes e imparciales en el ejercicio de sus funciones. Los Estados miembros deben notificar a la Comisión la identidad de esas autoridades competentes".*
[803] Artículo 17 del RGA

de datos específico de conformidad con el RGPD, y estará disponible de tal manera que permita su impresión en papel y que sea de fácil comprensión, así como en un formato electrónico y legible por máquina[804].

El Considerando 52 del RGA indica que, a fin de aportar confianza y seguridad jurídica adicional a la concesión o retirada del consentimiento, en particular, en el contexto de la investigación científica y la utilización estadística de los datos cedidos con fines altruistas, debe elaborarse un formulario europeo de consentimiento para la cesión altruista de datos y emplearse en el marco del intercambio de datos con fines altruistas. Para que en todo momento se tengan en cuenta las particularidades de los distintos sectores, especialmente desde la perspectiva de la protección de datos, el formulario deberá adoptar un diseño modular que permita su adaptación a sectores específicos y distintos fines. Esto es, gracias al diseño modular o ajustable que tendrá el formulario, podrá ser adaptado a sectores específicos y a distintos fines con el fin de adecuarlo a las particularidades de cada uno de los sectores.

A su vez, ha de estar redactado de una forma clara y sencilla, con el fin de que no se produzca ningún problema interpretativo por parte del interesado. Siguiendo la línea marcada por la Convención de Nueva York expuesta anteriormente, el formulario debería contemplar el caso particular de los interesados con discapacidad que quieran otorgar su consentimiento para la cesión altruista de sus datos. En consecuencia, en este formulario se ha de introducir un apartado relativo a la persona que presta el apoyo para que quede acreditado quien ha apoyado a la persona con discapacidad a la hora de otorgar su consentimiento.

La introducción del formulario puede ser tanto una oportunidad como un desafío para los investigadores. A primera vista, el formulario puede verse como un requisito más que ha de cumplirse para realizar el intercambio de los datos. Por otro lado, un formulario europeo uniforme de consentimiento para la cesión altruista de datos puede convertirse en una oportunidad para armonizar el consentimiento del interesado para el tratamiento de sus datos personales con fines de investigación y, por lo tanto, facilitar el intercambio de datos al menos dentro de la UE[805].

[804] Artículo 25 del RGA

[805] SHABANI, M., "The Data Governance Act and the EU's move towards facilitating data sharing", *Molecular Systems Biology*, Vol. 17, Núm.3, 2021, p. 2

CAPÍTULO 5: LOS DERECHOS DEL INTERESADO EN EL ÁMBITO SANITARIO

1. INTRODUCCIÓN:

En los capítulos anteriores nos hemos ocupado de indicar de qué manera pueden otorgar las personas mayores con discapacidad válidamente su consentimiento para el tratamiento de sus datos relativos a la salud en diversos contextos, en este capítulo abordaremos cómo pueden ejercer los derechos del interesado en el curso del tratamiento de sus datos relativos a la salud. Sabido es que siguiendo la tradición europea en materia de protección de datos, el Reglamento dedica un capítulo extenso a la nueva regulación de los derechos del interesado. Debido a la importancia que cobran estos derechos para la protección de datos personales del interesado, cabe preguntarse cómo han de ser interpretados y ejercidos en el ámbito específico de la salud y más concretamente de los datos relativos a la salud pertenecientes a las personas mayores, dado que su aplicación en un campo tan determinado puede crear interrogantes. Para lograr dicho objetivo, en el presente capítulo se estudiarán los derechos del interesado, desde los tradicionales hasta las nuevas incorporaciones.

Como consecuencia de la entrada en vigor del RGPD, el interesado ha visto como a los tradicionales derechos ARCO se han añadido el derecho al olvido, el derecho a la limitación del tratamiento y el derecho a la portabilidad de los datos personales. Los derechos ARCO quedan sustituidos por los derechos ARSLPO (acceso, rectificación, supresión e olvido, limitación del tratamiento, portabilidad y oposición) regulados entre los artículos 15 y 21 del RGPD. Este reforzamiento de los derechos ya existentes pretende adaptar los tradicionales derechos a la actual era digital. Igualmente, con la entrada en vigor del citado Reglamento, ha desaparecido la cancelación, sustituyéndose esta por el derecho de supresión o derecho al olvido. Por su parte, el artículo 22 del RGPD bajo el título "decisiones individuales automatizadas, incluida la elaboración de perfiles" regula el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en el interesado o le afecte significativamente de modo similar. Como se verá más adelante, no queda claro si se trata realmente de un derecho del interesado o una prohibición que introduce la normativa para el responsable del tratamiento de datos. Es por ello que no queda plasmado entre los derechos ARSLPO. Sin perjuicio de lo anterior, en este capítulo se analizará su contenido y lo que supone en el ámbito sanitario. Con esta ampliación de derechos, el RGPD ha pretendido reforzar la posición de control del interesado en cuanto a los mismos, al igual que ha reforzado los ya existentes[806].

Una vez se definido el ámbito de aplicación y alcance de los derechos de los interesados, se procederá a analizar su impacto el mundo de la salud digital, y lo que

[806] RODRÍGUEZ AYUSO, J.F., "Derechos del interesado como persona física propietaria de los datos personales", en GARCÍA ÁLVAREZ, L., *El mercado único en la unión europea*, Dykinson, Madrid, 2019, p. 220

estos nuevos derechos suponen para los pacientes, adentrándonos en el ámbito sanitario. Igualmente, a la hora de interpretar los derechos del interesado en este sector específico, se expondrán las diferencias que existen en determinados derechos en el caso de España, Italia e Irlanda. En este caso, incorporaremos un análisis de la normativa de desarrollo austriaca debido a su gran interés en materia de derechos digitales del paciente.

Finalmente, nos ocuparemos de analizar la problemática que suscita el ejercicio de estos derechos en el caso de las personas con discapacidad, teniendo en cuenta la nueva Ley 8/2021, y el proceso sancionador que se contempla en a normativa de protección de datos. En este punto se abordará también el caso particular del ejercicio de los citados derechos tras el fallecimiento del interesado en el ámbito sanitario, diferenciando para ello la aplicabilidad de los artículos 3 y 96 de la LOPDGDD. Para comprender adecuadamente la diferencia entre el acceso a los datos personales del fallecido, y el acceso *post mortem* de cualquier contenido en formato digital de la persona fallecida que regulan respectivamente los citados artículos, se analizarán las voluntades digitales de la normativa catalana y las directrices relativas al almacenamiento, supresión y comunicación de los datos personales de la normativa francesa. Para concluir, se tratará de responder a la pregunta de si el interesado puede reflejar su voluntad respecto a sus derechos relativos a la protección de datos personales para el caso en que fallezca en el documento de voluntades anticipadas.

2. LOS DERECHOS DEL INTERESADO:

2.1. El derecho de acceso:

2.1.1. Concepto:

Según el artículo 15 del RGPD, el interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen[807] y, en tal caso, podrá solicitar del responsable el acceso a los datos personales y a una serie de información adicional como los fines del tratamiento, las categorías de datos personales de que se trate y los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales.

Este derecho personalísimo e independiente, es reconocido a su vez en el artículo 8.2 de la Carta de los Derechos Fundamentales de la Unión Europea[808], y más concretamente, en el ámbito sanitario, en el artículo 18.1 de la LBAP[809] y en el artículo 12.1 del

[807] STJUE (Sala primera) de 10 de diciembre de 2010, (Land Nordrhein-Westfalen contra D.-H. T.), asunto C-620/19, ECLI:EU:C:2020:1011

[808] Artículo 8.2 de la Carta de los Derechos Fundamentales de la Unión Europea: "*toda persona tiene derecho a acceder a los datos recogidos que la conciernan y a su rectificación".*

[809] Artículo 18.1 de la LBAP: *"El paciente tiene el derecho de acceso, con las reservas señaladas en el apartado 3 de este artículo, a la documentación de la historia clínica y a obtener copia de los datos que*

Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica del País Vasco[810].

El derecho de acceso permite al interesado saber si alguien trata sus datos personales, para qué fines y cómo los trata, lo cual facilita al mismo tiempo, ejercer los restantes derechos reconocidos al interesado (rectificación, supresión e olvido, limitación del tratamiento, portabilidad y oposición). No en vano, es el conocimiento que le otorga el derecho de acceso el que le permite al interesado ejercer el resto de sus derechos. Así, el derecho de acceso se constituye como instrumento necesario para ejercer el resto de los derechos del grupo ARSLPO, como ha reconocido el TJUE en el caso Rijkeboer[811]. Sin perjuicio de lo anterior, es importante subrayar que, al tratarse de un derecho independiente, no es indispensable ejercerlo junto con los otros derechos.

En comparación con lo previsto anteriormente en el artículo 12 de la Directiva 95/46/CE y el artículo 15 de la LOPD, el Reglamento amplia el elenco de la información a la que el interesado puede acceder. Mediante la frase *"obtener el derecho de acceso a los datos personales y a la siguiente información",* en el artículo 15 del RGPD se pone de manifiesto que el derecho de acceso del interesado no solo se refiere a sus datos personales, sino que también se extiende a otra información como los fines del tratamiento o las categorías de datos personales de que se trate. Según el artículo 13.1 de la LOPDGDD, cuando el responsable trate una gran cantidad de datos relativos al afectado y este ejercite su derecho de acceso sin especificar si se refiere a todos o a una parte de los datos, el responsable podrá solicitarle, antes de facilitar la información, que el afectado especifique los datos o actividades de tratamiento a los que se refiere la solicitud.

Los interesados deben poder ejercitar su derecho de acceso con facilidad y a intervalos razonables. El RGPD no establece la forma en la que se proporcionará acceso a la

---

figuran en ella. Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos".

[810] Artículo 12.1 del Decreto 38/2012: *"De conformidad con lo dispuesto en el artículo 18 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, el o la paciente tiene el derecho de acceso a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Dicho derecho excluye el acceso a datos que deban limitarse por la existencia acreditada de un estado de necesidad terapéutica, del que el médico o la médica dejará constancia en la historia clínica. Dicho derecho asimismo no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en la historia clínica, recogidos en interés terapéutico de la persona paciente, ni en perjuicio del derecho de los y las profesionales participantes en su elaboración, quienes pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas".*

[811] Así se refería la STJUE (Sala tercera) de 7 de mayo de 2009, (College van burgemeester en wethouders van Rotterdam contra M. E. E. Rijkeboer), asunto C-553/07, ECLI:EU:C:2009:293, en su apartado 51 al indicar que: "*El citado derecho de acceso es indispensable para que el interesado pueda ejercer los derechos que se contemplan en el artículo 12, letras b) y c), de la Directiva, a saber, en su caso, cuando el tratamiento no se ajuste a las disposiciones de la misma, obtener del responsable del tratamiento de los datos, la rectificación, la supresión o el bloqueo de los datos [letra b)], o que proceda a notificar a los terceros a quienes se hayan comunicado los datos, toda rectificación, supresión o bloqueo efectuado, si no resulta imposible o supone un esfuerzo desproporcionado [letra c)]."*

información al interesado, indicando únicamente que el responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. Si el interesado ha presentado la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común. En este sentido, el artículo 13.2 de la LOPDGDD indica que el derecho de acceso se entenderá otorgado si el responsable del tratamiento facilita al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice de modo permanente el acceso a su totalidad.

En materia de los datos relativos a la salud, este derecho de acceso incluye el derecho de los interesados a acceder a datos relativos a la salud, por ejemplo, los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquiera tratamientos o intervenciones practicadas. Todo interesado debe tener el derecho a conocer y a que se le comuniquen los fines para los que se tratan sus datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento[812].

El derecho de acceso a la información sanitaria puede llegar a colisionar con otros derechos o intereses de otras personas o con otros bienes jurídicos que son también dignos de protección, como es el caso de los derechos de propiedad intelectual del médico en el caso de los historiales clínicos, haciéndose necesario limitar este derecho de acceso o, incluso, eliminarlo por completo, cuestión que será analizado en los siguientes puntos[813].

2.1.2. El acceso a la historia clínica por el paciente y sus límites:

En el ámbito sanitario, se ha dicho ya, se reconoce el derecho de los interesados a acceder a los datos relativos a la salud, a saber, los datos de sus historias clínicas que contengan información como diagnósticos, resultados de exámenes, evaluaciones de facultativos y cualesquier tratamiento o intervención practicada[814]. El derecho a la información responde a la obligación de los profesionales sanitarios de mantener informado en todo momento al paciente sobre su estado de salud y los tratamientos que se le aplican, y el derecho de acceso, responde a la facultad del usuario de conocer en un momento determinado el contenido de la historia clínica y demás documentación que contenga sus datos de carácter personal[815].

[812] Considerando 63 del RGPD
[813] RODRÍGUEZ AYUSO, J.F., *Garantía administrativa de los derechos del interesado en materia de protección de datos personales*, J.M. Bosch Editor, Barcelona, 2021, p. 56
[814] Considerando 63 de la LOPDGDD
[815] DE LORENZO MONTERO, R., Derechos y obligaciones de los pacientes: Análisis de la ley 41/2002, de 14 de noviembre básica reguladora de autonomía de los pacientes y de los derechos de información y documentación clínica, Colex, Madrid, 2003, p. 26

Por su parte, bajo la rúbrica de "usos de la historia clínica", la LBAP regula las diferentes finalidades o destinos de la documentación sanitaria, y determina qué persona, en cumplimiento de cada una de esas finalidades, puede acceder a la historia clínica. El artículo 16 de la LBAP se refiere a los usos de la historia clínica y el artículo 18 de la LBAP al derecho de acceso a la historia clínica, utilizando el término "uso" como sinónimo de finalidad, utilidad u objetivo, y el término "acceso" en el sentido de conocer, de obtener información. Los diferentes usos a los que está sujeta la historia clínica justifican cada uno de los supuestos de acceso, de forma que la legitimidad del acceso vendrá determinada por dos variables: el sujeto que accede y la finalidad o motivo del acceso. Asimismo, el motivo o finalidad del acceso es lo que delimita el alcance y extensión de este derecho[816].

Respecto a la solicitud de acceso en el ámbito sanitario, la LBAP no recoge un procedimiento específico, dejando en manos de los centros sanitarios la creación de dicho procedimiento[817]. El solicitado acceso ha de ser proporcionado al completo, es decir, el interesado ha de tener acceso a todo el historial clínico[818]. Por otra parte, el artículo 18.1 de la LBAP recoge que los pacientes tienen derecho a obtener copia de los datos que figuran en ella[819] en el plazo máximo de un mes[820].

En España cada una de las 17 autonomías ha establecido, normalmente medio de reglamentación administrativa, el procedimiento que deben seguir los pacientes para acceder a su expediente médico electrónico. En el País Vasco, por ejemplo, accediendo vía online a la "carpeta de salud"[821], los interesados pueden consultar y descargar informes (alta hospitalaria, quirúrgicos, de analítica, radiología, anatomía, patología, de atención primaria…), ver su historial farmacológico, ver el historial de vacunación, si está en la lista de espera quirúrgica, solicitar cita de atención primaria, incorporar informes externos a Osakidetza (reconocimientos médicos, análisis…), recibir notificaciones relacionados con programas de detección precoz de enfermedades

[816] SÁIZ RAMOS, M. y LARIOS RISCO, D., "El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas", *Derecho y salud*, Vol. 18, Núm. 1, 2009, p. 23

[817] Art 18.1 de la LBAP: *"Los centros sanitarios regularán el procedimiento que garantice la observancia de estos derechos".*

[818] El artículo 15.2 de la LBAP se refiere al contenido legal de la historia clínica de cada paciente.

[819] Véanse en este aspecto: resolución de la AEPD R/01773/2018 de 8 de enero de 2019 (Procedimiento núm. TD/01234/2018); resolución de la AEPD R/01620/2018 de 5 de octubre de 2018 (Procedimiento núm. TD/01026/2018) y resolución de la AEPD R/01463/2018 de 27 de agosto de 2018 (Procedimiento núm. TD/01032/2018).

[820]La resolución de la AEPD R/01583/2018 de 20 de septiembre de 2018 (Procedimiento Núm. TD/00946/2018) pone de manifiesto la importancia de cumplir con el plazo estipulado: "*En el supuesto aquí analizado, ha quedado acreditado que el reclamante ejercitó el derecho de acceso a copia íntegra de su historia clínica ante ASESMED y que, transcurrido el plazo establecido conforme a las normas antes señaladas, su solicitud no obtuvo la respuesta legalmente exigible (…) por todo ello, procede estimar, por motivos formales, la reclamación que originó el presente procedimiento de tutela de derechos al haberse satisfecho extemporáneamente el derecho sin que proceda la realización de actuaciones adicionales*."

[821] Es la puerta de entrada a la Historia Clínica Electrónica, en ella se almacena toda la información clínica y sanitaria de cada paciente del País Vasco.

o visualizar el documento de voluntades anticipadas en caso de tenerlo realizado[822]. Los interesados pueden acceder a su carpeta de salud mediante varios medios de identificación que pone a disposición del usuario Izenpe[823].

En Italia existe el "*fascicolo sanitario elettronico*" (FSE), regulado en el artículo 12 del Decreto Legislativo 179/2012 de 18 de octubre de 2012[824], el cual permite a los interesados acceder a sus datos relativos a la salud a través de las credenciales SPID (sistema público de identidad digital), CNS (tarjeta de servicio nacional) o CIE (tarjeta de identidad electrónica) en el portal del FSE de la región a la que correspondan. Es decir, aunque el artículo 12 regule el FSE, los datos de los interesados son proporcionados y gestionados por cada región. El FSE es generado tanto por estructuras de salud pública como privadas, y se posibilita que el interesado pueda introducir datos personales y documentos en el apartado del "cuaderno personal del paciente". Todos los accesos y operaciones que se hayan realizado dentro del FSE quedan registrados, y pueden ser notificados por correo electrónico al interesado[825].

En cuanto a Irlanda, no existe un "*electronic health record*" o historia clínica electrónica nacional, aunque sí que hay varios EHR para determinado sector poblacional: el sistema de gestión clínica materno y neonatal (MN-CMS), que ha implementado un EHR para todas las mujeres y bebés de las unidades de maternidad irlandesa, y el EHR de pacientes de epilepsia nacional irlandés (PiSCES). La mayor barrera para la creación de un EHR nacional es que Irlanda no tiene un identificador de salud individual (IHI)[826], ya que, aunque se creó la Ley 15/2014 de Identificadores de Salud de 2014 que entró en vigor el 8 de julio de 2014[827] para la introducción del identificador de salud individual, aún no se ha implementado por completo[828]. Debido a la falta de la historia clínica electrónica, los interesados deben completar el formulario de solicitud de acceso y enviarlo junto con una copia de su identificación con fotografía a su servicio de salud local[829].

A diferencia de los casos anteriores, en Austria existe el registro nacional "*elektronische Gesundheitsakte*" (ELGA), establecido por la Ley de telemática de la salud de 2012

---

[822] OSAKIDETZA., "Carpeta de salud", *osakidetza.euskadi.eus*, disponible en: https://www.osakidetza.euskadi.eus/servicios-on-line/-/carpeta-de-salud/ *[Última consulta: 2 de julio de 2022]*

[823] Autoridad de certificación vinculada al Gobierno Vasco.

[824] *"Decreto legge 18 ottobre 2012, n.179 Ulteriori misure urgenti per la crescita del Paese, GU n. 245 del 19 ottobre 2012"*

[825] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI., "Fascicolo sanitario elettronico (FSE)", 11 de enero de 2021, disponible en: https://www.garanteprivacy.it/temi/fse *[Última consulta: 2 de julio de 2022]*

[826] Número que se usará para identificar a una persona en el momento en que utiliza los servicios de atención sanitaria y social.

[827] "*15/2014 Health identifiers act 2014"*

[828] WALSH, B.; MAC DOMHNAILL, C. y MOHAN, G., "Developments in healthcare information systems in Ireland and internationally", *ESRI survey and statistical series*, Núm.105, 2021, pp. 40-43

[829] HSE., "Data Requests", disponible en: https://www.hse.ie/eng/gdpr/data-requests/ *[Última consulta: 4 de julio de 2022]*

(GTelG 2012)[830] y la Ordenanza ELGA 2015 de 12 de mayo de 2015[831], la cual ha tenido múltiples enmiendas. El sistema permite el acceso a los datos relativos a la salud de todo aquel que tenga acceso al sistema de salud austriaco, y su objetivo es complementar los tratamientos médicos y la consulta con mejores flujos de información, especialmente cuando varios proveedores de servicios de salud trabajan juntos. Los interesados pueden acceder a su historial clínico electrónico a través del portal ELGA registrándose con su firma digital o tarjeta de identificación electrónica, mediante lo cual se verifica su identidad. El sistema también muestra al interesado quién ha accedido a sus datos relativos a la salud y cuándo[832]. Todos los centros y hospitales públicos y farmacias de Austria participan en el ELGA[833].

El artículo 18.3 de la LBAP, al igual que el artículo 12.1 del Decreto 38/2012[834], dispone que el derecho al acceso del paciente a la documentación de la historia clínica no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en ella recogidos, en interés terapéutico del paciente, ni en perjuicio del derecho de los profesionales participantes en su elaboración, los cuales pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas. El primero de los límites no plantea ninguna duda, dado que es frecuente que en una historia clínica se incluyan anotaciones o datos relativos a terceras personas por ser una información trascendente que guarda relación con su estado de salud. En estos casos, esta información quedará fuera del alcance del derecho de acceso del paciente a su documentación clínica.

En cuanto al segundo, tal y como recoge el artículo 5.4 de la LBAP, el derecho a la información sanitaria de los pacientes puede limitarse por la existencia acreditada de un estado de necesidad terapéutica. Se entenderá por necesidad terapéutica la facultad del médico para actuar profesionalmente sin informar antes al paciente, cuando por razones objetivas el conocimiento de su propia situación pueda perjudicar su salud de manera grave. El profesional que advierte la existencia de un estado de necesidad terapéutica puede dejar fuera del alcance del conocimiento del paciente determinada información para evitar que el conocimiento de dicha información pueda generarle un daño o

[830] "*Gesundheitstelematikgesetzes 2012 (GTelG 2012), 14 dezember 2012, BGBl. I Nr. 111/2012"*
[831] *"ELGA-Verordnung 2015, 12 mai 2015, BGBl. II Nr. 106/2015"*
[832] ELGA., "About", *elga.gv.at*, disponible en: https://www.elga.gv.at/en/about-elga/ *[Última consulta: 6 de julio de 2022]*
[833] AUGUSTINOV, G. y DUFTSCHMID, G., "Can the Austrian nation-wide EHR system support the recruitment of trial patients?", *Studies in Health Technology and Informatics*, Núm. 259, 2019, p.87
[834] Artículo 12.1 del Decreto 38/2012: *"De conformidad con lo dispuesto en el artículo 18 de la Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, el o la paciente tiene el derecho de acceso a la documentación de la historia clínica y a obtener copia de los datos que figuran en ella. Dicho derecho excluye el acceso a datos que deban limitarse por la existencia acreditada de un estado de necesidad terapéutica, del que el médico o la médica dejará constancia en la historia clínica. Dicho derecho asimismo no puede ejercitarse en perjuicio del derecho de terceras personas a la confidencialidad de los datos que constan en la historia clínica, recogidos en interés terapéutico de la persona paciente, ni en perjuicio del derecho de los y las profesionales participantes en su elaboración, quienes pueden oponer al derecho de acceso la reserva de sus anotaciones subjetivas".*

perjuicio grave. Ahora bien, en este caso no puede hablarse de un "derecho" de reserva sino de una obligación o un deber de reserva de los profesionales sanitarios. Dicha obligación de reserva es una concreción del principio de no maleficencia[835], y coexiste con el respeto de la autonomía del paciente. Por consiguiente, ha de procurarse una armonización del principio de no maleficencia con el principio de autonomía[836].

El límite relativo a las anotaciones subjetivas suscita varios problemas. Por un lado, es preciso delimitar qué se entiende por anotaciones subjetivas. Por otro, también debe aclararse quién puede ejercer el derecho de reserva en relación con ellas[837]. La LBAP no define el término de anotaciones subjetivas, limitándose a mencionarlas en su articulado. Algunos legisladores autonómicos han abordado esta cuestión, aunque de forma contradictoria. En la Ley 3/2005, de 8 de julio de información sanitaria y autonomía del paciente de Extremadura, por ejemplo, se denomina anotaciones subjetivas a las impresiones de los profesionales sanitarios que, en todo caso, carecen de trascendencia para el conocimiento veraz y actualizado del estado de salud del paciente, sin que puedan tener la consideración de un diagnóstico[838].

En sentido contrario, en el artículo 7.4 del Decreto 38/2012 del País Vasco se entiende por anotaciones subjetivas las impresiones o valoraciones personales de las y los profesionales sanitarios no sustentadas directamente en datos objetivos o pruebas complementarias y que, en su criterio, resulten de interés para la atención sanitaria de la persona paciente. Igualmente, en el artículo 21.1 del Decreto 29/2009, de 5 febrero, por el que se regula el uso y acceso a la historia clínica electrónica de Galicia[839], se recoge que el personal sanitario deberá abstenerse de incluir expresiones, comentarios o datos que no tengan relación con la asistencia sanitaria del/de la paciente o que carezcan de valor sanitario. SÁNCHEZ-CARO y ABELLÁN[840] las definen como comentarios o impresiones personales que puede hacer el médico en un momento determinado, siempre que tengan trascendencia clínica, dado que en otro caso no deberían incluirse en el historial clínico.

Como se ha visto, las definiciones normativas y doctrinales discrepan en un punto fundamental, a saber, la trascendencia clínica o no de las anotaciones subjetivas. Muy

[835] El principio básico de bioética de no maleficencia se refiere a la obligación de no hacer daño intencionalmente. Se suele relacionar con la máxima hipocrática del "*primum non nocere"*, y recoge la obligación de no hacer daño junto a la de hacer el bien. Véase en este aspecto: PÁEZ MORENO, R., "La riqueza del principio de no maleficencia", *Cirujano General*, 2011, Vol. 33, Núm. S2, 2011, p. 178

[836] HERNANDO, P.; SEOANE, J.A. y DE ASÍS, J.F., "La reserva de las anotaciones subjetivas: ¿derecho o privilegio?", *Revista de calidad asistencial*, Vol. 21, Núm. 1, 2006, p.36

[837] GALLEGO RIESTRA, S., "Historia clínica electrónica y derecho a la autonomía del paciente: Un conflicto de intereses", *Papeles Médicos*, 2014, Vol. 23, Núm. 1, p. 9

[838] Art. 32.4.d) de la Ley 3/2005, de 8 de julio de información sanitaria y autonomía del paciente de Extremadura

[839] DOG núm. 34 de 18 de febrero de 2009

[840] SÁNCHEZ-CARO, J. y ABELLÁN, F., *Derechos y deberes de los pacientes: Ley 41/2002, de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas*, Comares, Granada, 2003, p. 75

acertadamente, GALLEGO RIESTRA[841] indica que las anotaciones subjetivas deben tener trascendencia clínica en todo caso. Según el autor, la inclusión en la historia de anotaciones subjetivas como meros juicios de valor solo tiene justificación si sirven para facilitar la asistencia del paciente. Así lo impone el propio tenor literal del artículo 15 de la LABP al señalar que la historia clínica deberá incorporar toda aquella información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente.

Respecto a la cuestión relativa a quiénes pueden oponer el derecho de reserva de las anotaciones subjetivas frente al derecho de acceso a la historia por parte del paciente, se considera que es un derecho de los profesionales que han realizado las mismas, y no de los centros[842]. La AEPD en su informe 0188/2011 de 9 de mayo de 2011 afirma que este derecho corresponde al propio facultativo, al tratarse de derecho personalísimo que únicamente incumbe al médico que introduce las supuestas anotaciones subjetivas en la historia clínica[843]. Asimismo, en la ya citada Resolución R/00633/2004 de 22 de noviembre de 2004, la AEPD afirmó que debe ser el facultativo quien realice las anotaciones subjetivas no la entidad.

A la hora de defender el derecho de reserva, en estrecha relación con el ya superado debate en torno a la propiedad de la historia clínica[844], se alega que las anotaciones subjetivas son propiedad intelectual del médico, y que se configuran, por tanto, como un componente creativo amparado bajo la ley de propiedad intelectual. El argumento decisivo para la delimitación de las anotaciones subjetivas es el elemento creativo que estas conllevan y que trasciende de la mera recopilación de datos obtenidos a través de pruebas o exámenes médicos, lo que implica la propiedad intelectual del médico sobre las mismas y el reconocimiento de su derecho moral como autor, en los términos en los que se contempla en la ley de propiedad intelectual[845].

En sentido contrario, según SERRATO MARTÍNEZ[846], no debería permitirse que el profesional sanitario pueda ejercer sus reservas a las anotaciones subjetivas, ya que esta opción implica una ruptura de la unidad de la historia clínica, integrada por el elemento objetivo y el subjetivo, y deja abierta la posibilidad de que el facultativo pueda retirar de la historia clínica los datos que pudieran perjudicarle ante una posible demanda por responsabilidad médica. Si se suprimen estas anotaciones, se estaría suprimiendo

[841] GALLEGO RIESTRA, S., "Historia clínica electrónica y derecho a la autonomía del paciente: Un conflicto de intereses", *cit.*, pp. 9-10
[842] SÁIZ RAMOS, M. y LARIOS RISCO, D., "El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas", *cit.*, p. 38
[843] SARRATO MARTÍNEZ, L., "El régimen legal de acceso a la historia clínica y sus garantías", *revista jurídica de castilla y león*, Núm. 17, 2009, p. 184
[844] Para mayor profundización: MARTÍNEZ HERNÁNDEZ, J., "Historia clínica", *Cuadernos de bioética*, Vol. 17, Núm. 1, 2006, p. 10
[845] DE LORENZO APARICI, O., "Problemática de las anotaciones subjetivas de la Ley 41/2002", *aeds*, 2006, p. 1, disponible en: https://www.aeds.org/congreso/congresos-aeds/ponencias/Ofelia%20de%20Lorenzo.pdf *[Última consulta: 9 de julio de 2022]*
[846] SARRATO MARTÍNEZ, L., "El régimen legal de acceso a la historia clínica y sus garantías", *cit.*, p. 184

aproximadamente un 90% de la historia clínica, por lo que se anularía el derecho primordial del paciente a acceder a los datos del documento, y supondría un perjuicio desde el punto de vista de la investigación o de una futura asistencia, ya que el historial puede tener trascendencia para abordar los futuros tratamientos de ese mismo paciente, por lo que deberían mantenerse en el historial clínico.

Si las anotaciones subjetivas no cumpliesen la finalidad principal de la historia clínica, la finalidad asistencial, u otra finalidad legítima reconocida en la LBAP, su presencia en la historia clínica no estaría justificada e implicaría un incumplimiento del deber de calidad de los profesionales sanitarios, debiendo ser suprimidas[847]. En consecuencia, será necesario que esta información se catalogue como elemento necesario del historial clínico, justificándose, en base al artículo 18.3 de la LBAP y el artículo 12.3 del Decreto 38/2012 la limitación del derecho de acceso del interesado[848].

Por otra parte, el derecho de acceso del paciente a los datos de su historia clínica tampoco comprende la información sobre los datos personales de las personas que, dentro del ámbito de organización del responsable del fichero, han podido tener acceso a la misma. Por consiguiente, salvo que una ley lo permita expresamente, el derecho de acceso a la historia clínica no incluye el derecho a saber quién ha consultado la misma[849]. Siguiendo esta línea, en el artículo 19.2 del Decreto 24/2011, de 12 de abril de la documentación sanitaria de la Castilla la Mancha se recoge que el derecho de acceso del paciente a los datos de su historia clínica no comprende la información sobre los datos personales de las personas que, dentro del ámbito de organización del responsable del fichero, han podido tener acceso a la misma en el ejercicio de sus funciones.

En un sentido contrario, el artículo 31.1 de la ley Foral 17/2010 de 8 de noviembre de derechos y deberes de las personas en materia de salud en la comunidad foral de Navarra indica que todas las personas tienen derecho a conocer en todo caso quién ha accedido a sus datos relativos a la salud, el motivo del acceso y el uso que se ha hecho de ellos, salvo en caso del uso codificado de los mismos.

Ante esta diversidad normativa, GALLEGO RIESTRA y RIAÑO GALÁN[850] llegan a afirmar que las interpretaciones restrictivas que propugnan la AEPD, el Ministerio de

[847] HERNANDO, P.; SEOANE, J.A. y DE ASÍS, J.F., "La reserva de las anotaciones subjetivas: ¿derecho o privilegio?", *cit.*, p.37

[848] El Valedor del Pueblo "Valedor do Pobo" de Galicia en su escrito a la Consejeria de Sanidad "Consellería de Sanidade" de 2 de noviembre de 2020 sobre el expediente núm. I.5.Q/2902/20, afirmaba que existía una situación de conflicto entre el derecho del paciente a obtener su historial clínico y el derecho del sanitario a la reserva de sus anotaciones subjetivas, ambos derechos con cobertura legal, y que carecía de competencias para establecer una ponderación y dirimir cuál de los dos derechos debía prevalecer. No obstante, consideró idóneo establecer algún mecanismo de revisión de las "anotaciones subjetivas" para poder garantizar que se ajustan al espíritu de la normativa en todos los casos.

[849] AEPD., Guía para pacientes y usuarios de la sanidad, *cit.*, p. 10

[850] GALLEGO RIESTRA, S. y RIAÑO GALÁN, I., "¿Tiene el paciente derecho a saber quiénes y por qué han accedido a su historia clínica?", *Derecho y salud*, Vol. 22, Núm. 1, 2012, p. 95

Sanidad[851] y alguna norma autonómica, no son más que trabas con escaso sustento legal y que tan solo conducen a una mayor judicialización de las relaciones de los ciudadanos con el sistema sanitario. En su opinión, salvo que los pacientes estén dispuestos a dejar en manos de cada centro sanitario la decisión sobre la legalidad de los accesos a sus historias clínicas, los pacientes solo tendrán derecho a acudir a la vía judicial para denunciar un posible acceso ilegitimo. Por ello, es necesaria según esta doctrina una norma que posibilite a los pacientes saber quién ha realizado cada uno de los accesos a su historia clínica.

Recuérdese finalmente que, en determinadas ocasiones, puede negarse el derecho de acceso al paciente por seguridad de la comunidad o del Estado, como es el caso de las epidemias o enfermedades que puedan poner en riesgo la estabilidad de la ciudadanía en general. En el artículo 23.1 del RGPD se recoge la limitación de los derechos del interesado para salvaguardar la seguridad del estado, la defensa, la seguridad pública, la prevención, la investigación, la detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, los objetivos importantes de interés público general de la Unión o de un Estado miembro (económicos, financieros etc.) y la protección de la independencia judicial y de los procedimientos judiciales entre otros. Para estos fines, se aplicarán medidas proporcionadas en base al Derecho de la Unión o del Estados miembro aplicables al responsable o al encargado del tratamiento. De la misma manera, en los apartados 2 y 3 del artículo 89 RGPD se recoge la posibilidad de limitar los derechos del interesado, entre ellos el derecho de acceso, en los supuestos en los que el tratamiento de los datos personales persiga fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, siempre que dichas limitaciones sean totalmente necesarias para alcanzar los citados fines.

2.1.3. El acceso a la historia clínica electrónica por los profesionales sanitarios:

El acceso a la historia clínica como tal se considera un tratamiento de datos de carácter personal relativos a la salud[852]. Para poder realizar dicho tratamiento, se necesita una base legal, que en el ámbito de la asistencia sanitaria será la recogida en el artículo 9.2.h) del RGPD. En el mismo sentido, el artículo 16.1 de la LBAP establece que los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de este como instrumento fundamental para

[851] El Ministerio de Sanidad ha creado la Historia Clínica Digital del Sistema Nacional de Salud (HCDSNS), cuyo objetivo es establecer una historia clínica compartida que posibilite su uso por los centros asistenciales de España que atiendan a un mismo paciente. Su implantación se encuentra en estos momentos en fase de prueba en diferentes Comunidades Autónomas. Así, en la página web del Ministerio de Sanidad encontramos un documento que explica el funcionamiento de esta herramienta. En su página 47, apartado en el que explica la información que aportará el sistema sobre cada acceso efectuado, no se recoge la opción de saber quién realizó cada uno de los accesos. INSTITUTO DE INFORMACIÓN SANITARIA., "El sistema de historia clínica digital", *mscbs*, disponible en: https://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf

[852] AEPD Informe jurídico núm. 2021/0038, de 17 de junio de 2020

su adecuada asistencia. Por ello, se entiende que la historia clínica es un elemento inherente e imprescindible de la asistencia sanitaria que se presta[853].

Esta necesaria concurrencia de una finalidad asistencial para justificar el acceso a los datos relativos a la salud del paciente es lo que se conoce como principio de vinculación asistencial. Este principio está unido al principio de proporcionalidad, que determina que el profesional debe acceder únicamente a los datos mínimos necesarios para prestar la asistencia sanitaria concreta. Todas aquellas incursiones que sobrepasen los límites por ellos marcados habrán de ser consideradas injustificadas, a menos que se encuentren amparadas por alguna de las otras finalidades previstas en el artículo 16 de LBAP[854].

Tal y como señala el Informe Jurídico de la AEPD nº 0656/2008 de 7 de enero de 2009, como regla general, el acceso a la historia clínica en el ámbito de un determinado centro sanitario quedará limitado al propio personal que preste la asistencia al paciente. El citado informe hace una referencia especial al personal de enfermería indicando que, en base a la Ley 44/2003 de 21 de noviembre de Profesiones Sanitarias, tienen la condición de personal sanitario, y que, en consecuencia, podrán acceder al historial clínico del paciente para garantizar una asistencia adecuada al mismo, y en tanto los datos de la historia constituyan un "instrumento fundamental para su adecuada asistencia" en cada caso concreto. Se ha de estar, así, a un análisis de las funciones propias de cada una de las categorías, de lo que derivará la necesidad o no de acceso a la historia, al ser esta instrumental para la realización de sus funciones[855].

A título de ejemplo, el Decreto 38/2012 del País Vasco ha sido más preciso a la hora de regular el procedimiento de acceso por profesionales de los centros y servicios sanitarios con finalidad asistencial. En su artículo 13 se regula el acceso a la documentación de la historia clínica por el personal de los centros o servicios sanitarios, que tendrá un carácter selectivo en consideración a la categoría profesional, al tipo de datos y al lugar o puesto de trabajo en relación con los procesos asistenciales realizados, y se introduce la obligación de que las Instituciones titulares de los centros o servicios sanitarios tengan aprobadas instrucciones claras al respecto. Los facultativos solo pueden acceder a los datos clínicos necesarios para el diagnóstico y tratamiento[856].

---

[853] SOCIEDAD ESPAÑOLA DE SALUD PÚBLICA y ADMINISTRACIÓN SANITARIA., "Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD", *sespas*, 2017, p. 52, disponible en: https://sespas.es/wp-content/uploads/2018/02/SESPAS_informe_proteccion_datos_2017.pdf

[854] SALUD CASANOVA ASENCIO, A., "Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias", *cit.*, p. 7

[855] STSJ de Castilla y León Sala de lo contencioso 862/2018, de 28 de febrero de 2018 (Rec. Núm. 210/2018)

[856] En este sentido, a modo de ejemplo, puede indicarse que el obstetra debe saber que el feto de una mujer embarazada es fruto de un óvulo donado, pero esta misma información es irrelevante para el traumatólogo ante un esguince de tobillo. En consecuencia, el traumatólogo no deberá tener acceso a dicha información para realizar su diagnóstico. Véase al respecto: BELTRÁN AGUIRRE, J. L., "La protección de los datos personales relacionados con la salud", cit., p. 62

Con el fin de garantizar este acceso restringido, el Decreto vasco establece que los sistemas de información de la historia clínica de los centros sanitarios deberán identificar de forma inequívoca y personalizada a todo profesional que intente acceder a la información contenida en la historia clínica de una persona como paciente o persona usuaria y verificarán su autorización. Se deberá dejar constancia, además, de cualquier acceso en términos que permitan tener conocimiento de la persona que accede, la fecha y la finalidad, debiéndose guardarse de cada intento de acceso como mínimo la identificación del profesional, fecha, hora, la parte de la historia clínica a la que se ha accedido y el tipo de acceso. Cuando el acceso sea denegado por no cumplir los criterios de acceso, la propia denegación deberá quedar también registrada[857]. El control de los accesos deberá efectuarse de la forma más detallada posible, a fin de conocer efectivamente quién ha podido en cada momento conocer los datos incorporados al sistema, es decir, a qué datos o recursos se ha accedido, sin que puedan efectuarse meros controles genéricos, por referencia al sistema en su conjunto. Por consiguiente, el responsable deberá tener las aplicaciones informáticas necesarias que permitan cumplir con esta exigencia[858].

Como corolario de esta tensión entre el derecho de acceso del paciente, el derecho de reserva y acceso del clínico, puede señalarse que la aceptabilidad de un sistema de tratamiento de datos con un potencial de riesgo excepcional, depende de la existencia de un nivel suficientemente elevado de seguridad en el conjunto del sistema. Esta seguridad se traduce en que el acceso por parte de personas no autorizadas debe ser técnicamente imposible. El marco jurídico por el que se crea un sistema de historia clínica digital debería prever la aplicación de una serie de medidas técnicas y organizativas destinadas a evitar la pérdida de datos o la alteración, tratamiento y acceso no autorizados[859]. El profesional sanitario que acceda ilícitamente a datos de salud puede incurrir en un delito de descubrimiento y revelación de secretos, previsto y penado en el artículo 197 del Código Penal. La sentencia del Tribunal Supremo de 23 de septiembre de 2015 condenó a un médico por el delito de descubrimiento y revelación de secretos que, aprovechando su condición de médico y utilizando su número de usuario y contraseña personal, entró en veinticinco ocasiones a las historias clínicas de pacientes de sus compañeros sin autorización y sin que mediara relación asistencial entre ellos[860].

2.1.4. El acceso a la historia clínica electrónica para actividades de gestión, inspección, y planificación de los servicios sanitarios:

El acceso a los datos de la historia clínica con fines administrativos por parte de profesionales no clínicos es necesario para garantizar el soporte administrativo que el proceso asistencial precisa, por lo que será legítimo que el personal de administración y

[857] Artículo 13.2. del Decreto 38/2012
[858] AEPD Informe jurídico núm. 0584/2009 de 21 de enero de 2010
[859] GT29. Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 15 de febrero de 2007, p. 21
[860] STS Sala de lo Penal 532/2015, de 23 de septiembre de 2015 (Rec. Núm. 648/2015)

gestión pueda acceder a las historias clínicas. Sin embargo, la normativa establece que para garantizar el derecho a la protección de datos del paciente, el acceso por parte del personal de administración y gestión solo se realizará en el entorno del ejercicio de sus funciones, de manera que no dispondrán de todos aquellos datos confidenciales que no les resulten necesarios para el cumplimiento de sus cometidos[861].

Los centros sanitarios deberán difundir los procedimientos y protocolos necesarios para que todo el personal, tanto el profesional sanitario como el administrativo, conozca cuáles son sus funciones y sus atribuciones con respecto al tratamiento de los datos contenidos en las historias clínicas. En el mismo sentido, los responsables de las historias clínicas deben establecer diferentes niveles de acceso en atención a las funciones que desempeñen las personas que tengan que acceder a las historias clínicas con fines distintos a los asistenciales (gestión de citas, derivaciones, etc.)[862].

El artículo 16.5 de la LBAP, autoriza al personal sanitario debidamente acreditado el acceso a la historia clínica para desarrollar las funciones de inspección sanitaria, evaluación y acreditación de servicios sanitarios en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria[863].

2.1.5. Acceso a la historia clínica por terceros con fines de docencia:

El artículo 16.3 de la LBAP prevé la posibilidad de acceder a la historia clínica de los pacientes con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, pero obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que como regla general no se pueda identificar al interesado, salvo que el mismo haya dado su consentimiento para no separarlos.

Una vez analizado en el capítulo anterior el tratamiento de datos personales con fines de investigación sanitaria, durante la pandemia producida por el COVID-19 y el tratamiento con fines de salud pública, en este punto nos centraremos en el ámbito del acceso de terceros al historial clínico con fines de docencia.

Según Orden SSI/81/2017, de 19 de enero, por la que se publica el Acuerdo de la Comisión de Recursos Humanos del Sistema Nacional de Salud, por el que se aprueba el protocolo[864] mediante el que se determinan pautas básicas destinadas a asegurar y

[861] Artículo 16.4 de la LBAP
[862] SARRATO MARTÍNEZ, L., "El régimen legal de acceso a la historia clínica y sus garantías", *cit.*, p. 197
[863] En el mismo sentido se refiere el artículo 15 del Decreto 38/2012
[864] El objetivo del presente protocolo es establecer pautas básicas de actuación destinadas a garantizar el derecho a la dignidad e intimidad del paciente cuando es atendido en presencia de alumnos de titulaciones relacionadas con las ciencias de la salud (alumnos) y cuando es atendido por profesionales que cursan formación especializada en Ciencias de la Salud (residentes en formación).

proteger el derecho a la intimidad del paciente por los alumnos y residentes en Ciencias de la Salud[865], la disociación de datos obliga a separar los datos clínico-asistenciales de aquellos otros que permitan identificar a su titular (número de historia clínica, de la Seguridad Social, DNI, etc.)[866]. La disociación de datos habrá de realizarla un profesional sanitario sujeto al secreto profesional u otra persona sujeta a una obligación equivalente de secreto. En el ámbito de la docencia los alumnos podrán acceder a la historia clínica con datos personales disociados o historias clínicas simuladas por el responsable de docencia a fin de garantizar que el aprendizaje derivado de las mismas se realiza respetando la intimidad y confidencialidad de los datos de salud[867].

La dirección del Centro autorizará el acceso al registro de la historia clínica, requiriendo para ello el informe previo y motivado del tutor o los responsables de la investigación/máster/título propio/doctorado que se someterá a dictamen previo del correspondiente Comité de Ética Asistencial/Investigación. Dicha autorización tendrá los límites temporales que se adecuen a la finalidad concreta para la que se autoriza el acceso[868]. Los alumnos estarán supervisados en todo momento, y no podrán acceder a la información clínica del paciente sin la supervisión directa del personal del centro asistencial que sea responsable de su formación[869].

Por su parte, el artículo 16 del Decreto 38/2012 del País Vasco establece que se podrá acceder a la historia clínica con fines de investigación; docencia; estudio epidemiológico o de salud pública; dirección, planificación o programación del sistema sanitario; facturación de servicios sanitarios y judiciales. Asimismo, al igual que la normativa estatal, la norma vasca estipula que el acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del o de la paciente separados de los de carácter clínico-asistencial, de manera que como regla general quede asegurado el anonimato, salvo que la propia persona paciente haya dado su consentimiento para no separarlos, exceptuándose los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos de la propia persona paciente con los clínico-asistenciales. En estos casos se estará a lo que dispongan los Jueces o Juezas y Tribunales en el proceso correspondiente.

[865] Orden SSI/81/2017, de 19 de enero, por la que se publica el Acuerdo de la Comisión de Recursos Humanos del Sistema Nacional de Salud, por el que se aprueba el protocolo mediante el que se determinan pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente por los alumnos y residentes en Ciencias de la Salud (BOE núm. 31 de 6 de febrero de 2017).

[866] En este marco, el artículo 15.4 del Código Deontológico de la Organización Médica Colegial (OMC) indica que el análisis científico y estadístico de los datos contenidos en las historias clínicas y la presentación de algunos casos concretos pueden proporcionar informaciones muy valiosas, por lo que su publicación es autorizable desde el punto de vista deontológico, pero el paciente no podrá ser reconocible o identificable.

[867] Punto 7.2.1 del Protocolo

[868] Punto 7.2.2 del Protocolo

[869] Punto 5.4 del Protocolo

2.2. Derecho de rectificación:

2.2.1. Concepto:

Tal como exige el principio de exactitud de los datos recogido en el artículo 5.1.d) del RGPD, el responsable debe velar por que los datos sean exactos y estén actualizados. Sin embargo, cuando los datos sean inexactos o estén desfasados, el interesado puede acudir al derecho de rectificación. Recogido en los artículos 16 del RGPD y 14 de la LOPDGDD, se refiere al derecho que tiene el interesado de instar al responsable del tratamiento a que rectifique sus datos personales cuando estos sean inexactos o sean incompletos en atención a la finalidad del tratamiento o finalidades del tratamiento. Es decir, el interesado puede instar al responsable del tratamiento a que, por una parte, rectifique los datos personales que sean inexactos y, por otra parte, atendiendo a la finalidad o finalidades del tratamiento, a que complete sus datos personales[870]. Mediante este derecho, se garantiza la exactitud de los datos y, por tanto, el tratamiento lícito de los mismos.

Se ha dicho con acierto que la exactitud de los datos personales es esencial para garantizar un alto nivel de protección de los datos de los interesados[871]. Por este motivo, cuando se trate de datos inexactos, la normativa recoge que el responsable del tratamiento deberá rectificar los mismos sin dilación indebida, aunque esta obligación no impide que el responsable pueda pedir al interesado que proporcione documentos o información que acrediten dicha inexactitud. Asimismo, cuando el interesado ejerce su derecho de limitación del tratamiento por comprender que los datos no son exactos, el responsable dispondrá de un plazo para verificar la exactitud de los mismos. Por tanto, la expresión "sin dilación indebida" tiene sus matices.

Si la rectificación tiene por objeto completar los datos incompletos, el interesado tendrá derecho a que se realice dicho acto incluso. El objetivo de la declaración adicional es proporcionar al responsable del tratamiento los datos personales necesarios que falten para que los datos sean completos. Se deberá analizar si los datos personales del interesado son los estrictamente necesarios para cumplir la finalidad o finalidades del tratamiento.

En base al artículo 32 del LOPDGDD, se deberán bloquear los datos, identificándolos e impidiendo su tratamiento, incluso su visualización, mientras no se haya resuelto la solicitud de rectificación. En los casos en que la configuración del sistema de información no permita el bloqueo o se requiera una adaptación que implique un esfuerzo desproporcionado, se procederá a un copiado seguro de la información de modo que conste evidencia digital o de otra naturaleza, que permita acreditar la autenticidad de la misma, la fecha del bloqueo y la no manipulación de los datos.

[870] APARICIO SALOM, J. y VIDAL LASO, M., *Estudio sobre la protección de datos, cit.,* p. 77
[871] CdE. *Manual de legislación europea de protección de datos, cit.,* p. 247

En suma, la inexactitud o las carencias del dato objeto de tratamiento pueden ser objeto del derecho de rectificación del interesado, que puede provocar la supresión del dato antiguo y su sustitución por el nuevo o la complementación del mismo. Este derecho se convierte en una obligación a cumplir por el responsable del tratamiento en el caso de que se observe la existencia de datos incompletos o inexactos[872].

2.2.2. El derecho de rectificar los datos relativos a la salud inexactos o incompletos:

La LBAP no contiene ninguna referencia explícita al derecho de rectificación, aunque en su artículo 15 se establece que la historia clínica incorporará la información que se considere trascendental para el conocimiento veraz y actualizado del estado de salud del paciente. Si los datos son incorrectos o inexactos, el profesional sanitario no dispondrá "de un conocimiento veraz y actualizado del estado de salud de su paciente" como requiere la norma. El empleo de datos erróneos por parte de los profesionales sanitarios puede acarrear riesgos para la salud de los pacientes, puesto que se tomarían decisiones en base a información no verídica. Por ejemplo, si en el historial clínico de un paciente se indica un tipo de sangre distinto al suyo, puede realizarse una transfusión de sangre entre grupos incompatibles que le causaría una respuesta inmunitaria grave, es por ello que el presente derecho cobra una especial importancia en el ámbito sanitario.

Por tanto, el paciente que compruebe que la información contenida en su historial clínico no es correcta o esté incompleta, tendrá el derecho de solicitar la rectificación[873]. Una vez realizada la solicitud de rectificación, corresponderá al profesional sanitario determinar si debe rectificarse el dato o no. Los profesionales sanitarios han de analizar las circunstancias de cada caso, siempre desde el criterio médico, para valorar si este cambio puede condicionar o perjudicar la asistencia sanitaria al paciente. Nótese que este deber no es personalizado sino que corresponde, en general, a los centros sanitarios que deben analizar las circunstancias de cada caso, desde la perspectiva del criterio médico y del interés terapéutico del paciente[874].

A pesar de la importancia del derecho de rectificación en el ámbito de la sanidad, pueden crearse ciertas situaciones problemáticas como consecuencia del ejercicio del mismo, por ejemplo, cuando los datos del historial clínico fueron ciertos en un pasado, pero no lo son en la actualidad. Para saber si se puede llevar a cabo la rectificación, se deberá analizar si dicha rectificación perjudicará la asistencia sanitaria del mismo interesado o de terceras personas. En este sentido, la AEPD en su informe jurídico 0268/2011 de 1 de septiembre de 2011, analizó el caso de una mujer transexual que

[872] REBOLLO DELGADO, L. y SERRANO PEREZ M.M., *Introducción a la protección de datos*, Dykinson, Madrid, 2008, p. 210

[873] Resoluciónes de la AEPD: R/01422/2018 de 8 de octubre de 2018 (Procedimiento núm. TD/01051/2018), R/00847/2018 de 18 de mayo de 2018 (Procedimiento núm. TD/00297/2018), R/00858/2018 de 18 de mayo de 2018 (Procedimiento núm. TD/00296/2018) y R/01455/2018 de 27 de agosto de 2017 (Procedimiento núm. TD/00917/2018).

[874] APDCAT. Guia de protecció de dades per a pacients i usuaris dels serveis de salud, *cit.*, p. 13

solicitaba modificar el género y nombre en los episodios de su historia clínica acaecidos mientras aún era hombre. Así, en el citado informe, se cuestiona el derecho de rectificación que tienen los pacientes transexuales de modificar su nombre en todos los episodios de sus historias clínicas.

La AEPD resolvió esta cuestión afirmando que, si bien la información contenida en la historia clínica debe figurar en su denominación bajo el nombre actual de los pacientes, los concretos episodios recogidos en la misma, deberán conservar la información necesaria que garantice a los facultativos saber que, los pacientes en el momento de desarrollarse dichos episodios eran del género contrario. Se negó el derecho de rectificación de la interesada alegando que el conocimiento de dicha información por parte de los facultativos era necesario para otorgarle una asistencia sanitaria adecuada en el futuro. Por todo ello, para poder conceder el derecho de rectificación se deberá analizar si dicha rectificación perjudicará en el futuro la asistencia sanitaria del mismo interesado o de terceras personas[875].

2.3. Derecho de supresión:

2.3.1. Concepto:

Aunque en muchas ocasiones se hable de los derechos de supresión y olvido como si se tratasede conceptos sinónimos, en realidad, no son estrictamente el mismo derecho. Con el título de "derecho de supresión («el derecho al olvido»)" del artículo 17 del RGPD, el propio legislador mueve a confusión, puesto que al introducir entre paréntesis y comillas el derecho al olvido, parece que se trata de una denominación común del derecho a la supresión, equivalente en todo a aquél. Sin embargo, como se verá, las diferencias entre ambos son sustanciales. Veamos en primer lugar en qué consiste el derecho de supresión.

El derecho de supresión constituye la versión renovada del antiguo derecho de cancelación. Se trata del derecho que tienen los ciudadanos de solicitar al responsable del tratamiento la eliminación de sus datos personales cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; el interesado retire el consentimiento en que se basa el tratamiento de los datos; el interesado se oponga al tratamiento; los datos personales hayan sido tratados ilícitamente; los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información[876]. En palabras del Consejo de Europa, es especialmente importante asegurar el derecho de los interesados

[875] ALKORTA IDIAKEZ, I., El espacio europeo de datos sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios, *cit.*, pp. 58-59

[876] STJUE (Sala Cuarta), de 27 de octubre de 2022, Proximus NV contra Gegevensbeschermingsautoriteit, ECLI:EU:C:2022:833

a la supresión de sus propios datos para la aplicación efectiva de los principios de protección de datos, y en particular del principio de minimización de datos[877].

Al ejercer este derecho, se obliga al responsable a que cese el tratamiento de los datos personales y que lleve a cabo el borrado de los mismos. Como sabemos, en base al artículo 32 del LOPDGDD, mientras no se haya resuelto la solicitud se deberán bloquear los datos, identificándolos e impidiendo su tratamiento.

2.3.2. La supresión de los datos relativos a la salud:

El derecho a la supresión en el ámbito sanitario supone que los pacientes tendrán derecho a solicitar "el borrado" de sus datos relativos a la salud[878]. No obstante, se limita el derecho a la supresión de datos de la historia clínica por motivos de asistencia sanitaria, tratamiento sanitario o interés público en el ámbito de la salud[879], ya que es cierto que el médico y personal clínico no podrían atender adecuadamente al paciente si parte de su historial clínico pudiera ser borrado a instancias del paciente y por su sola voluntad. Se debe tener en cuenta que el historial clínico tiene un fuerte impacto y puede no ser apropiado eliminar una entrada del mismo[880]. Esto puede deberse a razones legales, tanto para la protección del paciente como de las personas involucradas en el tratamiento del paciente, pero también para garantizar que los futuros profesionales de

[877] CdE. *Manual de legislación europea de protección de datos*, *cit.,* p. 249

[878] Este derecho es aplicable a todo el ámbito sanitario. Así, el artículo 15.3 de la Ley Orgánica 11/2021, de 28 de diciembre, de lucha contra el dopaje en el deporte en el deporte recoge que los y las deportistas serán informados en el momento de recibir la notificación del control y, en su caso, al iniciarse la recogida de la muestra, de los derechos y obligaciones que les asisten en relación con el citado control, de los trámites esenciales del procedimiento y de sus principales consecuencias, del tratamiento y cesión de los datos previstos en la presente ley, así como de la posibilidad de ejercitar los derechos de acceso, rectificación, supresión y oposición, establecidos en el RGPD.

[879] AEPD., Guía para pacientes y usuarios de la sanidad, noviembre, *cit*., p.7

[880] El caso Yvonne Chave contra Francia es un ejemplo clásico de la limitación del derecho a la supresión en el ámbito de la salud. Con fecha de 17 de diciembre de 1970, Yvonne fue internada en un hospital psiquiátrico hasta mayo de 1971. Posteriormente, el 6 de noviembre de 1978, el Tribunal de Apelación de París, resolvió que el internamiento había sido ilegal y ordenó que la recurrente fuera indemnizada con 5.000 francos dado que el internamiento, por la forma en la que se realizó, había supuesto un menoscabo grave para la misma teniendo en cuenta que la Sra. Chave era muy conocida en la localidad de Carpentras. La recurrente, consideró que la indemnización no era suficiente para reparar el daño sufrido y solicitó que sus datos personales fueran borrados del registro central de los pacientes con enfermedad mental del Departamento de Vaucluse y de cualquier otro registro. Al ver que su solicitud había sido denegada, acudió al Tribunal Administrativo de Marsella. El Gobierno Francés alegó que el propósito de estos documentos era proteger la salud y los derechos de los pacientes. Asimismo, declaró que el acceso a los ficheros estaba estrictamente regulado, pudiendo acceder a los mismos únicamente las autoridades públicas en el ejercicio de sus poderes. Mediante resolución de fecha 10 de febrero de 1983, el Tribunal Administrativo de Marsella rechazó la solicitud alegando que, la solicitante no había probado que la información almacenada le provocase ningún perjuicio, puesto que, según el Tribunal, solamente podría causarle algún perjuicio si dicha información se divulgara. Ante esta situación, la Sra. Chave apeló ante el Consejo del Estado (Conseil d'Êtat), quien sostuvo la postura del Tribunal Administrativo de Marsella. El Consejo realizó una ponderación de los intereses en conflicto, concluyendo que la injerencia que había sufrido la Sra. Chave no había sido desproporcionada respecto al fin perseguido: la protección de su salud. Por ello, el Consejo del Estado consideró que no procedía la supresión por motivos de asistencia sanitaria. Véase al respecto: STEDH 14461/88, de 9 de julio de 1991 asunto Yvonne Chave née Jullien contra Francia

la salud tengan disponibles todos los datos que puedan influir en el tratamiento que se le aplique al paciente.

Para el cumplimiento de los citados fines, la normativa establece un plazo mínimo de conservación. El artículo 19.1 del Decreto 38/2012, al igual que el artículo 17.1 de la LBAP, obliga a los centros sanitarios a conservar la documentación clínica de los pacientes en un plazo mínimo de 5 años desde la fecha del alta de cada proceso asistencial. Este plazo de 5 años de conservación es aplicable, entre otras, a las hojas clínico-estadísticas, las hojas de autorización de ingreso, las hojas de evolución y planificación de cuidados de enfermería, las hojas de aplicación terapéutica, las hojas de gráficas de constantes y las hojas de urgencias[881]. Sin embargo, las hojas de informes clínicos de alta, las hojas de alta voluntaria, las hojas de consentimiento informado, las hojas de informes quirúrgicos y/o de registro del parto, las hojas de anestesia, las hojas de informes de exploraciones complementarias y las hojas de informes de necropsia serán conservadas de manera definitiva[882].

Como norma general, los datos personales contenidos en las historias clínicas deberán conservarse durante un plazo mínimo de cinco años[883], no procediendo la supresión de dichos datos cuando pudiera perjudicarse la salud del paciente al que se refieren los mismos, sin olvidar otros intereses legítimos de terceros[884]. En el plazo de esos cinco años, los datos relativos a la salud informatizados podrán ser bloqueados, imposibilitando así su tratamiento, pero no suprimidos. El bloqueo implica la identificación y reserva de los datos fuera de los circuitos de trabajo ordinarios y la adopción de medidas que impidan el tratamiento. En el caso de que estos datos se encuentren almacenados en soporte papel, este procedimiento se realizará mediante el almacenamiento de los ficheros correspondientes en un lugar diferenciado.

En otros ordenamientos, el bloqueo se ha entendido de forma ligeramente distinta. En Irlanda, siguiendo lo estipulado en el artículo 17 del RGPD, se permite el ejercicio del derecho de supresión en el ámbito sanitario pero no de una forma absoluta, cada solicitud debe examinarse y considerarse de forma individual[885], respetando en todo momento los plazos de conservación que se indican en el "*HSE Records Retention Policy*" o política de retención de los datos del servicio de salud irlandés.

En el caso de Italia, los interesados no pueden suprimir los datos personales del FSE, en cambio, pueden solicitar la ocultación de datos relativos a la salud y documentos

[881] Artículo 10 del Decreto 45/1998 de 17 de marzo, por el que se establece el contenido y se regula la valoración, conservación y expurgo de los documentos del Registro de Actividades Clínicas de los Servicios de Urgencias de los Hospitales y de las Historias Clínicas Hospitalarias.
[882] Artículo 11 del Decreto 45/1998
[883] Artículo 17.1 de la LBAP y artículo 19.1 del Decreto 18/2012
[884] AEPD. Resolución R/00847/2018 de 18 de mayo de 2018 (Procedimiento núm. TD/00297/2018)
[885] HSE., "General Data Protection Regulation (GDPR) Frequently asked questions (Faqs)", *hse*, p.4, disponible en: https://www.hse.ie/eng/gdpr/gdpr-faq/hse-gdpr-faqs-public.pdf *[Última consulta: 22 de julio de 2022]*

sanitarios del mismo[886]. Los datos y documentos pueden ocultarse, pero no eliminarse por completo, debiendo permanecer accesibles para la parte que generó los datos, generalmente el médico tratante[887].

En cuanto a Austria, el artículo 16.2.a) de la Ley de telemática de la salud va más allá que las anteriores, y contempla una doble posibilidad: la ocultación y la supresión. Los interesados pueden a su elección ocultar o eliminar sus datos relativos a la salud, incluyendo información relativa a medicamentos, de ELGA siempre que no lo impidan otras obligaciones legales referidas a la obligación de mostrar el expediente completo en los procesos judiciales y en otras situaciones en las que se impone el interés superior de un tercero. Si el interesado ha optado por ocultar sus datos, estos pueden ser nuevamente "visibles" si así lo decide más adelante, sin embargo, los datos que hayan sido suprimidos no se pueden recuperar, esta acción es irrevocable[888].

En España la AEPD recuerda que el derecho fundamental a la protección de datos personales no es absoluto, ni prevalece en cualquier caso ante otros intereses o derechos, pudiendo ser objeto de tratamiento los datos de carácter personal cuando resulte necesario para la prevención o para el diagnóstico médicos, la prestación de la asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios. Ello implica que en determinados supuestos en los que la ley legitima o incluso impone el tratamiento, no es posible realizar la supresión de los datos personales como resultado de la solicitud del interesado[889]. Aunque dicha realidad puede conllevar un perjuicio para el interesado, todos los derechos tienen que convivir con otros derechos y la seguridad de la sociedad. Por tanto, el derecho a la supresión de datos no es ilimitado y aplicable en todo caso.

2.4. El derecho al olvido:

2.4.1. Concepto:

Reconocido en el artículo 17 del RGPD, el derecho al olvido se define como la manifestación de los derechos de cancelación y oposición aplicados a los buscadores de

[886] El Garante impuso una sanción pecuniaria administrativa por el valor de 120.000€ a la Autoridad Sanitaria Local de Emilia-Romaña mediante la Orden judicial del Garante contra la Autoridad Sanitaria Local de Emilia-Romaña de 27 de mayo de 2021 (núm. 211) por transmitir, a través de la red de información regional, al médico de cabecera un informe que la interesada había pedido que se ocultara. Aunque la interesada había solicitado expresamente que se ocultara el informe que recogía que había interrumpido voluntariamente su embarazo, debido a un error informático se envió la notificación de su hospitalización a su médico de cabecera, motivo por el cual se impuso la sanción declarando la ilicitud del tratamiento de datos personales.

[887] GARANTE PER LA PROTEZIONE DEI DATI PERSONALI., "Fascicolo sanitario elettronico-Domande più frequenti", *garanteprivacy*, disponible en: https://www.garanteprivacy.it/faq/fascicolo-sanitario *[Última consulta: 23 de julio de 2022]*

[888] ELGA., "Schulungsunterlagen: Textbausteine zur Ergänzung und Unterstützung eigener Schulungsunterlagen", *elga.gv.at*, 16 de febrero de 2016, p. 19, disponible en: https://www.elga.gv.at/fileadmin/user_upload/Dokumente_PDF_MP4/Technisches/ELGA_Basis_fuer_Schulungsunterlagen_V2.0.pdf

[889] AEPD. Informe Jurídico núm. 189/2003 de 4 de agosto de 2003

Internet[890], y hace referencia al derecho de impedir la difusión de información personal a través de internet cuando su publicación no cumple los requisitos de adecuación y pertinencia previstos en la normativa. En concreto, incluye el derecho a limitar la difusión universal e indiscriminada de datos personales en los buscadores generales cuando la información es obsoleta o ya no tiene relevancia ni interés público, aunque la publicación original sea legítima (en el caso de boletines oficiales o informaciones amparadas por las libertades de expresión o de información)[891]. Se trata de una herramienta mediante la cual los interesados pueden controlar su información personal que se encuentra en Internet[892]. El legislador estatal contempla el reconocimiento de este derecho en dos artículos, diferenciando el derecho al olvido en búsquedas de Internet del derecho al olvido en servicios de redes sociales y servicios equivalentes[893], lo cual evidencia el valor del derecho al olvido en el ámbito de estas últimas.

Según MARTÍNEZ OTERO[894], el reconocimiento del derecho al olvido recuerda el surgimiento del derecho a la intimidad a finales del XIX y principios del XX. Aquel derecho, que en sus primeras formulaciones fue descrito como el derecho a ser dejado en paz (“*to be let alone”)*, respondía a los avances tecnológicos y a los hábitos de comunicación de aquella época, que permitían la captación de la vida íntima de las personas y su reproducción masiva (cámaras de fotos y de vídeo, micrófonos, extensión de la prensa escrita). El avance tecnológico ha derribado las barreras naturales de tiempo y espacio que protegían a las personas frente al conocimiento permanente por terceros de hechos o circunstancias que pueden perjudicarles en el desarrollo de su vida. La duración de la información en Internet constituye una amenaza para el libre desarrollo de la personalidad[895], puesto que Internet registra todo y no olvida nada[896]. En este sentido, es interesante observar el término inglés del derecho al olvido “*the right to be forgotten*”, puesto que significa literalmente “el derecho a ser olvidado”.

El valor temporal de la información es una de las principales bases del derecho al olvido[897]. Por ello, el derecho al olvido está muy inspirado en conceptos como el

---

[890] STJUE (Gran Sala), de 24 de septiembre de 2019, C-136/17, ECLI:EU:C:2019:773

[891] APCPD., “Derecho al olvido”, apcpd, disponible en: https://www.apcpd.es/derecho-al-olvido/ *[Última consulta: 25 de julio de 2022]*

[892] Debido a la era digital en la que vivimos, se ha puesto de manifiesto la necesidad de desarrollar reglas transnacionales de protección de datos personales, incluyendo diseños del derecho al olvido, lo cual permitirá que el derecho a la protección de datos personales siga siendo un derecho protegido en la era digital. Véase al respecto: FABBRINI, F. y CELESTE, E., “The right to be forgotten in the digital age: the challenges of data protection beyond borders”, *German law journal*, Vol. 21, Núm. S1, 2020, p. 65

[893] Artículos 93 y 94 de la LOPDGDD

[894] MARTÍNEZ OTERO, J.M., “El derecho al olvido en internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja”, *Revista de derecho político*, Núm. 93, 2015, p. 106

[895] MIERES MIERES, L.J., *El derecho al olvido digital*, Fundación Alternativas, Madrid, 2014, p. 6

[896] ROSEN, J., “The web means the end of forgetting”, *nytimes*, 21 de Julio de 2010, disponible en: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html *[Última consulta: 26 de julio de 2022]*

[897] El elemento “temporal” es central, distinguiéndolo de otros ejercicios de ponderación que también imponen límites o contornos específicos a la libertad de expresión. Véase al respecto: LETURIA INFANTE, F.J., “Fundamentos jurídicos del derecho al olvido: ¿un nuevo derecho de origen europeo o una respuesta típica ante colisiones entre ciertos fundamentos?”, *Revista chilena de derecho*, Vol. 43, Núm. 1, 2016, p. 92

perdón y la reinserción social del ámbito penal[898], una vez que hayas pagado tu deuda con la sociedad, se ha de tener una segunda oportunidad. Asimismo, se identifica otra noción extraída de la política penal: un plazo de prescripción[899], pasado un determinado tiempo, los delitos prescriben[900].

Lo que se pretende mediante el derecho al olvido es que los datos personales no sean indexados por los buscadores, aunque esto no implica que las páginas deban ser eliminadas. Las URL-s (direcciones web) dejarán de ser visibles cuando la búsqueda se realice mediante el dato del interesado que ejerció su derecho al olvido. Por ejemplo, si en una determinada página web figura el nombre del interesado y este quiere que al poner su nombre en cualquier buscador no se derive a la página en cuestión, mediante el derecho al olvido, la URL dejaría de estar visible no pudiendo acceder con el nombre del interesado a dicha página. No obstante, al no borrarse la página, se podrá acceder a la misma por otros medios.

Se aplica en las mismas circunstancias que el derecho de supresión, pero cuando el tratamiento de los datos personales se realiza en Internet. Esto es, según el Reglamento, este derecho se aplica cuando el tratamiento se lleve a cabo en Internet y los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo; el interesado retire el consentimiento en que se basa el tratamiento de los datos; el interesado se oponga al tratamiento; los datos personales hayan sido tratados ilícitamente; los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, o los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información. No puede decirse que se trate de un derecho distinto, la función y la aplicabilidad es la misma, solo cambia el "lugar" o ámbito de aplicación.

Según ÁLVAREZ CARO[901], el derecho al olvido podría definirse como el derecho a equivocarse o a que una equivocación pasada no marque y determine la vida de un

[898] Esta idea se refleja en el caso de los asesinatos de Apollonia. En el año 1982, se produjo una doble muerte a manos de un tripulante del barco Apollonia en plena travesía, hecho que conmocionó a la sociedad alemana. La noticia estuvo por todas partes durante meses, hasta se creó un documental y se publicó un libro sobre el caso. El hombre fue condenado a cadena perpetua, quedando en libertad en el año 2002. Al salir de la cárcel, veinte años más tarde de que se produjeran los hechos, el ex presidario descubrió que, al realizar una búsqueda con su nombre en internet, se encontraba información sobre el caso en una revista digital, quedando su nombre asociado a estos asesinatos. A partir de ese momento, comenzó un camino judicial para que esa información no se indexara a su nombre, ejerciendo para ello su derecho al olvido. En el año 2012, el Tribunal Federal de Justicia (Bundesgerichtshof) rechazó su petición alegando que la información era de interés público. Posteriormente, el Tribunal Constitucional Federal de Karlsruhe reconoció el derecho al olvido del apelante alegando que, dada la antigüedad, esa información no era de interés público. Véase al respecto: Sentencia del Tribunal Constitucional Federal alemán 1 BvR 16/13, de 6 de noviembre de 2019.

[899] En un sentido contrario: AUSLOOS, J., "The Right to be Forgotten, a Worth remembering?", *Computer Law & Security Review*, Vol. 28, Núm. 2, 2012, p. 149

[900] SHEFET, D., "The right to be forgotten", *Scitech Lawyer*, Vol. 16, Núm. 3, 2020, p. 27

[901] ÁLVAREZ CARO, M., *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital*, *cit.*, pp. 68-69

individuo que, por definición, no es otra cosa que un proceso evolutivo, una secuencia de aciertos y errores, siempre en proceso de conformación, de cambio y de evolución constante. En este mismo sentido, señala SIMON CASTELLANO[902] que resulta desproporcionado seguir difundiendo determinada información cuando carece de interés público o actualidad, en la medida que mantiene al afectado en la tribuna pública contra su voluntad. Como permite proteger el interés de las personas a obtener el olvido digital de datos del pasado que les puedan perjudicar, este derecho tiene una estrecha relación con el respeto del libre desarrollo de la personalidad y con bienes sustantivos, la intimidad y el honor.

Desde otra óptica, MIERES[903] opina que el derecho al olvido no es el producto del mero capricho de las personas a que su pasado no sea conocido, sino que responde a una necesidad sentida por los ciudadanos de poder controlar la trazabilidad de su vida digital y poder eliminar, o limitar la difusión, de aquellos aspectos cuya accesibilidad permanente puede incidir negativamente, entre otros, en su carrera laboral, su crédito o sus relaciones sociales. El establecimiento de equilibrios razonables en los supuestos de conflicto es la vía adecuada para preservar los intereses contrapuestos de acceder libremente a toda la información en línea y de precaverse frente al conocimiento permanente de informaciones pasadas que perjudican al interesado.

En una posición contraria, SALVADOR CODERCH[904] alega que la censura retroactiva de los medios de información es la cara oscura del pretendido derecho al olvido. Según el autor, su consagración legal produciría efectos perversos e imprevistos por muchos de sus proponentes; realimentaría nuestros prejuicios, perpetuándolos, en lugar de permitirnos encararlos y superarlos con humanidad; y reforzaría a las élites del poder, las cuales podrían seguir accediendo a los archivos en su soporte originario, agrandando la brecha entre poderosos y desapoderados.

Por último, recogemos la opinión de VINT CERF[905], el cual manifestó que el derecho al olvido puede ser una amenaza para la web**.** Este autor afirma que los ciudadanos no pueden eliminar contenidos alojados en la nube o en ordenadores particulares solo por querer que el mundo se olvide de una información. Haciendo una comparación, el autor dice que ejercer el derecho al olvido sería como tratar de quitar un determinado libro de las estanterías de los ciudadanos para que estos no puedan leer lo que está escrito en el

[902] SIMÓN CASTELLANO, P., *El reconocimiento del derecho al olvido digital en España y en la UE: efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, Barcelona, 2015, p. 105
[903] MIERES MIERES, L.J., *El derecho al olvido digital*, *cit.*, p. 51
[904] SALVADOR CODERCH, P., "Entre recordar y olvidar", *elpaís* 1 de junio de 2011, disponible en: https://elpais.com/diario/2011/06/01/opinion/1306879205_850215.html *[Última consulta: 28 de julio de 2022]*
[905] WARMAN, M., "Vint Cerf attacks European internet policy", *telegraph*, 29 de marzo de 2012, disponible en: https://www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html *[Última consulta: 29 de julio de 2022]*

mismo. En el mismo sentido, FLEISCHER[906] alega que la historia debe recordarse, no olvidarse, incluso si es dolorosa, puesto que la cultura es memoria.

En este punto, es de interés citar el caso Google Spain, S.L. y Google Inc contra la AEPD y Mario Costeja González[907], puesto que esta sentencia del TJUE sentó las bases del derecho al olvido. Tras la digitalización de la hemeroteca de un determinado periódico, el nombre de Mario Costeja apareció ligado a una subasta por un embargo a causa de deudas, las cuales habían sido pagadas hacía tiempo, hecho que reflejaba la carencia de relevancia actual de la noticia según el interesado. El TJUE resolvió que teniendo en cuenta el carácter sensible de la información para la vida privada de esta persona y de que su publicación inicial se remontaba a 16 años atrás, no parecían existir razones concretas que justificaran un interés preponderante del público en tener acceso a esta información en el marco de tal búsqueda[908]. Por todo lo antedicho, el derecho al olvido no es un derecho absoluto, en cuanto que puede ser limitado por otros derechos con los que puede entrar en conflicto, de ahí la necesidad de ponderar en cada caso para determinar la prevalencia de uno u otro[909]. Es preciso hacer una valoración caso por caso, para determinar si el derecho al olvido es aplicable o no[910].

A su vez, el TJUE indicó que el ejercicio del derecho solo afecta a los resultados obtenidos en las búsquedas hechas mediante el nombre de la persona y no implica que la página deba ser borrada de los índices del buscador. Es decir, una cosa es el derecho a que se olvide el enlace que dirige a la información y otra distinta que esta vaya a desaparecer de la red[911]. En consecuencia, la información no se borrará de la web original y seguirá siendo accesible a través del buscador por cualquier otra palabra o término que no sea el nombre del afectado. Respecto a esta cuestión, puede alegarse que al no obligar a los editores web el borrado de la información, el derecho al olvido puede devenir ineficaz. En este aspecto puede afirmarse que el hecho de no otorgar ningún tipo de responsabilidad al editor web imposibilita una protección eficaz y completa, ya

[906] FLEISCHER, P., "The right to be forgotten, or how ti edut your history", *pteterfleischer.blogspot*, 29 de enero de 2012, disponible en: http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html *[Última consulta: 29 de julio de 2022]*

[907] STJUE (Gran Sala) de 13 de mayo de 2014, Google Spain, S.L. y Google Inc. contra la AEPD y Mario Costeja González, asunto C-131/12, ECLI:EU:C:2014:317

[908] En el apartado 81 de la sentencia se indica que el derecho a la protección de datos de las personas prevalece, con carácter general, sobre el interés económico del gestor del motor de búsqueda y el interés del público a acceder a la mencionada información, aunque, en el mismo apartado se defiende que es preciso buscar un justo equilibrio entre los derechos. Volviendo al ya citado caso de Apollonia, aunque en un principio la publicación de dicha información hubiese sido de interés, es defendible que, transcurrido un espacio de tiempo tan amplio, la información dejó de tener interés público y que la libertad de información no se vio afectada al reconocer el derecho al olvido.

[909] BERROCAL LANZAROT, A.I., *Derecho de supresión de datos o derecho al olvido*, Reus, Madrid, 2017, p. 243

[910] ÁLVAREZ CARO, M., *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital*, *cit*., p. 108

[911] CASARES MARCOS, A. B., "Derecho al olvido en internet y autodeterminación informativa personal: el olvido está lleno de memoria", *Revista de administración pública*, núm. 212, 2020, p. 423

que se podrá seguir accediendo a la información por otras vías[912]. Aunque Google sea uno de los buscadores más utilizados, eliminar un dato del buscador de Google no es eliminar un dato de Internet[913].

2.4.2. El derecho al olvido en el ámbito sanitario:

En el ámbito sanitario, cuando el paciente quiera proceder al borrado de sus datos personales, en la gran mayoría de los casos, realmente se ejercerá el derecho de supresión y no el derecho al olvido puesto que los datos relativos a la salud de los pacientes no se encuentran a disposición de los ciudadanos en Internet. No obstante, pueden crearse situaciones en las que el paciente podrá ejercer el derecho al olvido en este ámbito.

Un ejemplo del ejercicio de este derecho en el ámbito sanitario puede ser la solicitud de borrado de las imágenes del "antes y después" de un paciente. Así, si una persona con una enfermedad cutánea autoriza la publicación de sus imágenes faciales antes y después del tratamiento recibido en una clínica dermatológica, tras cambiar de opinión, puede solicitar que se eliminen de la página web dichas fotografías. Estas imágenes serían datos personales puesto que, al mostrar la cara del paciente, permitirían establecer la identidad del interesado. A su vez, indicarían que el mismo padece o padecía una enfermedad cutánea, lo cual es un dato relativo a la salud que pertenece a la categoría especial de datos personales. En un principio su tratamiento sería lícito al contar con el consentimiento del interesado, pero este último podría solicitar su eliminación en base al artículo 17.1.c) del RGPD.

Otro caso ejemplificativo es el que fue objeto de una impugnación ante la Agencia de Protección de Datos. La AEPD sancionó a un centro hospitalario por llevar a cabo entre mediados de abril de 2016 y principios de agosto de 2018 un tratamiento de datos relativos a la salud sin previo consentimiento al publicar en su página web el contenido íntegro de una carta de agradecimiento remitida por el reclamante al hospital con motivo del tratamiento psicológico que recibió en el mismo, apareciendo reseñados en dicha publicación los datos identificativos y la condición de paciente del reclamante. El interesado fue informado por familiares de que a través del buscador de internet Google, introduciendo el nombre y apellidos del mismo, se podía acceder a dicha carta de agradecimiento, quedando de manifiesto que recibió un tratamiento psicológico en

---

[912] ÁLVAREZ CARO, M. *Derecho al olvido en internet: el nuevo paradigma de la privacidad en la era digital, cit*., p. 117-118

[913] En el caso Google contra *Commission nationale de l'informatique et des libertés* (CNIL), el TJUE resolvió que "*cuando el gestor de un motor de búsqueda estime una solicitud de retirada de enlaces en virtud de estas disposiciones, estará obligado a proceder a dicha retirada no en todas las versiones de su motor, sino en las versiones de este que correspondan al conjunto de los Estados miembros, combinándola, en caso necesario, con medidas que, con pleno respeto de las exigencias legales, impidan de manera efectiva o, al menos, dificulten seriamente a los internautas que efectúen una búsqueda a partir del nombre del interesado desde uno de los Estados miembros el acceso, a través de la lista de resultados que se obtenga tras esa búsqueda, a los enlaces objeto de la solicitud de retirada*". Véase al respecto: STJUE de 24 de septiembre de 2019, Google contra CNIL, C-507/17, ECLI:EU:C:2019:772

dicho centro[914]. Gracias a este derecho, la publicación de la página web del hospital fue eliminada. En este caso, el derecho al olvido era aplicable debido a que los datos personales del interesado estaban siendo tratados ilícitamente, puesto que no había otorgado su consentimiento.

2.5. Derecho a la limitación del tratamiento de datos:

2.5.1. Concepto:

El artículo 18 del RGPD introdujo un nuevo derecho al elenco de los derechos reconocidos al interesado en la anterior Directiva. Se define como un derecho mediante el cual el interesado podrá solicitar al responsable del tratamiento la limitación temporal del tratamiento de sus datos personales. La LOPDGDD lo regula en su artículo 16, aunque remite a lo legislado en el citado artículo del RGPD. El artículo 4.3 RGPD lo define como el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro, debiendo constar claramente en los sistemas de información del responsable el hecho de que el tratamiento está limitado.

Se trata de un derecho que permite al interesado, cuyos datos personales son objeto de tratamiento, solicitar al responsable del tratamiento que aplique medidas sobre unos datos personales para, entre otras cosas, evitar su modificación o, en su caso, su borrado o supresión, otorgando al interesado mayor control sobre sus datos personales. En consecuencia, es una medida cautelar que reduce el tratamiento de los datos personales a la conservación[915] que tiene su antecedente en el derecho al bloqueo[916] previsto en la derogada Directiva 95/46/CE.

El artículo 18.1 del RGPD recoge los cuatro supuestos en los que el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos[917]. El primer supuesto se refiere a que, el interesado, cuyos datos personales son objeto de tratamiento, pueda impugnar ante el responsable del tratamiento la exactitud de los datos. Cuando el interesado ejerza esta impugnación, el responsable tendrá que limitar su tratamiento y verificar su exactitud. La limitación del tratamiento se realizará

[914] AEPD. Resolución procedimiento sancionador núm. PS/00404/2018 de 23 de diciembre de 2019

[915] CAMPOS ACUÑA, C., *Aplicación práctica y adaptación de la protección de datos en el ámbito local: novedades tras el reglamento europeo; el consultor de los ayuntamientos*; Wolters Kluwer, Madrid, 2018, p. 163

[916] El artículo 12.b) de la Directiva recogía el derecho a bloqueo cuando el tratamiento no se ajustara a la disposiciones de la directiva, en particular cuando los datos fueran incompletos o inexactos.

[917] Artículo 18.1 del RGPD: *"El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:*
a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado".

durante un plazo que permita al responsable verificar la exactitud de los datos personales, por lo cual, se entiende que el responsable deberá actuar sin dilación indebida y, en cualquier caso, en el plazo de un mes[918].

El segundo supuesto contempla el caso de que el tratamiento de los datos personales que lleva a cabo el responsable del tratamiento sea contrario a derecho. En este caso, el interesado podrá solicitar la limitación del tratamiento de sus datos para que el responsable no pueda suprimir los mismos. Con este segundo supuesto, el legislador ha tratado de crear una medida destinada a que se conserve la prueba de la infracción cometida por el responsable del tratamiento.

También se puede aplicar este derecho cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones. Es decir, cuando el responsable del tratamiento ya no necesita los datos, pero el interesado los necesite para llevar a cabo reclamaciones o defenderse de ellas. Una vez ejercido el derecho, el responsable del tratamiento deberá seguir manteniendo los datos personales del interesado.

Por último, el cuarto supuesto se refiere al caso en el que el interesado se haya opuesto al tratamiento de sus datos ejercitando su derecho de oposición cuando dicho tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o para la satisfacción de intereses legítimos. Por tanto, mediante la limitación de este tratamiento se verificará si las razones que legitiman el tratamiento de los datos personales por el responsable del tratamiento prevalecen al derecho fundamental a la protección de datos personales del interesado.

Tanto en el Considerando 68 como en el artículo 16.2 del LOPDGDD se indica que, cuando el interesado solicite la limitación del tratamiento de sus datos, esta solicitud deberá constar claramente en los sistemas de información del responsable para que mientras dure esta limitación el responsable tenga en todo momento presente dicha limitación y no pueda realizarse ningún tratamiento de los datos por equivocación.

Corresponderá al responsable del tratamiento aplicar las medidas para limitar el tratamiento de los datos personales del interesado. Respecto al modo en el que se realizará dicho acto, el Considerando 67 del RGPD recoge que entre los métodos para limitar el tratamiento de datos personales cabe incluir los consistentes en trasladar temporalmente los datos a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos personales seleccionados o en retirar temporalmente los datos personales publicados de un sitio web. En los ficheros automatizados, la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse.

[918] Artículo 12.3 del RGPD

En el supuesto en que la limitación se haya hecho efectiva, el responsable del tratamiento comunicará la limitación del tratamiento efectuada a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El problema surge en el momento de valorar si su ejercicio realmente es imposible o exige un esfuerzo desproporcionado, labor que quedará en manos de la jurisprudencia. En cualquier caso, el responsable deberá de informar al interesado acerca de dichos destinatarios, si este así lo solicita[919]. Antes de que se levante la limitación, el responsable deberá informar a todo interesado que haya obtenido la limitación del tratamiento que se procederá con el preceptivo levantamiento.

Cuando concurran cualquiera de las cuatro circunstancias descritas, y el interesado haya ejercido su derecho a la limitación del tratamiento, dichos datos solo podrán ser objeto de tratamientocuando el interesado haya otorgado su consentimiento; para la formulación, el ejercicio o la defensa de reclamaciones; para la protección de los derechos de otra persona física o jurídica; o por razones de interés público importante de la Unión o de un determinado Estado miembro[920].

2.5.2. La limitación del tratamiento de los datos relativos a la salud:

En determinados casos en que exista un conflicto entre un paciente y un centro sanitario, el paciente podrá ejercer el derecho a limitar el tratamiento, es decir, podrá solicitar que sus datos personales no sean tratados, a saber, mientras el centro decide sobre la exactitud de los datos; cuando el paciente desea que los datos se conserven incluso si el tratamiento puede ser ilícito o innecesario; cuando el responsable del tratamiento ya no necesita los datos, pero el paciente los necesita para llevar a cabo reclamaciones o defenderse de ellas; y mientras el centro decide si el derecho de oposición es aplicable[921].

Es preciso observar que, en el primer y cuarto caso señalados, convergen dos derechos distintos del interesado. En cuanto al primero, concurren en el tiempo el derecho de rectificación y el derecho a la limitación del tratamiento. Si un paciente considera que sus datos personales no son exactos y solicita la rectificación de los mismos, se limitará el tratamiento de los datos mientras se decide sobre su exactitud. En consecuencia, ante la solicitud del paciente, se deberá averiguar si realmente ese dato personal es erróneo o no, debiendo limitar el tratamiento mientras el centro decide sobre la exactitud del mismo.

En el último caso, entran en juego el derecho de oposición y el derecho a la limitación del tratamiento del paciente. Cuando el paciente ejerza su derecho de oposición porque no quiere que sus datos relativos a la salud sean tratados para un determinado fin, se

[919] Artículo 19 del RGPD
[920] Artículo 18.2 del RGPD
[921] APDCAT. Guia de protecció de dades per a pacients i usuaris dels serveis de salud, *cit.*, p.19

limitará el tratamiento de dichos datos hasta que se sepa si los motivos del responsable prevalecen sobre los del interesado, realizándose una ponderación.

2.6. Derecho a la portabilidad de los datos:

2.6.1. Concepto:

El artículo 20 del RGPD, tras un largo debate parlamentario, introdujo el derecho a la portabilidad de datos[922]. Gracias a este derecho, el interesado, puede recibir en un formato estructurado, de uso común y lectura mecánica los datos que proporcionó anteriormente al responsable del tratamiento, y transmitirlos a otro responsable del tratamiento sin impedimentos[923]. No solo posibilita la obtención y reutilización de sus datos personales al interesado, sino que hace posible la transmisión de los citados datos a otro responsable del tratamiento. Se ha dicho con acierto que este derecho tiene una doble vertiente, puesto que se refiere al derecho del interesado a recibir sus datos en formato estructurado, de uso común, de lectura mecánica e interoperable; y por otra parte, al derecho del mismo a exigir al responsable la transmisión de los datos a otro responsable del tratamiento[924].

De una forma simplificada podemos definirlo como el derecho que ostenta el interesado a que el responsable del tratamiento le "devuelva" sus datos personales. Una vez tenga en su poder nuevamente estos datos personales, el interesado tendrá la opción de "transmitir" los mismos a otro responsable. También se permite la transmisión directa, pudiendo ser los datos personales trasladados por el primer responsable al segundo sin pasar por las manos del interesado[925]. Su objetivo primordial es mejorar el control que tienen los interesados sobre sus datos personales y garantizar que desempeñen un papel activo en el ecosistema de datos[926]. Respalda la elección, el control y la capacitación de

[922] Es a su vez recogido en el artículo 17 de la LOPDGDD

[923] Es descrito como una experiencia sin fronteras donde las personas pueden moverse fácilmente entre servicios de red, reutilizar los datos que proporcionan mientras controlan su privacidad y respetan la privacidad de los demás. Véase al respecto: VAN DER AUWERMEULEN, B., "How to attribute the right to data portability in Europe: A comparative analysis of legislations", *Computer law & security review*, Vol. 33, Núm.1, 2017, p. 58

[924] CAMPOS ACUÑA, C., *Aplicación práctica y adaptación de la protección de datos en el ámbito local: novedades tras el reglamento europeo; el consultor de los ayuntamientos, cit.*, p. 156

[925] Por ejemplo, un cliente de un banco, que por determinadas razones quiera cambiarse de sucursal, podrá solicitar al responsable la transmisión de sus datos personales. Igualmente, tendrá opción de solicitar la transmisión directa, mediante la cual, los datos pasarán directamente al segundo banco.

[926] Se ha de diferenciar el derecho a la portabilidad de los datos, de los anteriormente analizados derechos de acceso y derecho a la supresión. En cuanto al derecho de acceso, podría sostenerse que se trata de un derecho de "conocimiento", mientras que el derecho a la portabilidad es un derecho de "control". Asimismo, el artículo 20 del RGPD, delimita la aplicabilidad del derecho a la portabilidad al hablar de datos que se encuentren en un formato de lectura mecánica, mientras que el artículo 15 del mismo cuerpo legal, referido al derecho del acceso, no habla de ningún determinado formato. Respecto al derecho a la supresión, el Considerando 68 RGPD recoge que el derecho a la portabilidad no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato. Así, la portabilidad de los datos no conlleva automáticamente el borrado de los datos de los sistemas del responsable del tratamiento. Cuando el interesado ejerciendo su derecho a la portabilidad

los usuarios, reequilibrando la relación entre los interesados y los responsables del tratamiento[927]. Sin embargo, aunque el objetivo primordial sea mejorar el control que tienen los individuos sobre sus datos personales, no es menos cierto que la creación de este derecho se basa en el deseo de promover la libre circulación de los datos personales en el territorio europeo, promoviendo igualmente la competencia entre los responsables del tratamiento[928].

En este sentido, según la profesora Isabel GONZÁLEZ PACANOWSKA, se trata de un derecho de carácter económico, pero se conecta con el derecho de acceso, y no es reflejo de un derecho patrimonial de disposición sobre los datos personales. La portabilidad hay que interpretarla también en clave económica de mercado, puesto que permita garantizar la libre competencia, pero no como manifestación de un poder patrimonial exclusivo y excluyente del titular como sería el derecho de propiedad[929].

2.6.2. Portabilidad de los datos personales que el interesado "haya facilitado":

De conformidad con el artículo 20.1 del RGPD, los datos personales objeto de este derecho serán aquellos datos personales que incumban al interesado y que hayan sido facilitados por la misma. Respecto a la primera condición, dado que los datos han de incumbir al interesado, se excluyen los datos que se encuentren anonimizados, pero sí se incluyen aquellos datos personales que estén seudonimizados.

Respecto a la segunda condición, el Grupo de Trabajo del artículo 29 se decanta por una interpretación no restrictiva al afirmar que la expresión "facilitados por el interesado" debe interpretarse en un sentido amplio y se han de excluir los "datos inferidos" y los "datos deducidos", que incluyen los datos personales generados por un proveedor de servicios, por ejemplo, resultados algorítmicos[930]. Es decir, los datos personales pueden considerarse como datos facilitados por el interesado cuando han sido proporcionados por el interesado de una manera consciente y activa (por ejemplo, los datos enviados a

---

solicite al responsable la transmisión de sus datos a otro responsable, el primero, una vez realizada la transmisión, no borrará directamente dichos datos. Posteriormente, si el interesado quisiera borrar sus datos de la base de datos de este primer responsable tendría que ejercitar su derecho de supresión. Véase al respecto: KIVE, M. y GRASIS, J., "Problems of application of the right to data portability", *Acta Prosperitatis*, núm.11, 2020, pp. 118-119

[927] GT29. Directrices sobre el derecho a la portabilidad de los datos, 16/ES (WP 242 rev.01), 13 de diciembre de 2016, p. 4

[928] La portabilidad de los datos personales es un elemento esencial de la economía digital, ya que los desarrollos públicos y privados reposan cada vez en mayor medida en la disposición de datos en formatos que permitan la interoperabilidad de los sistemas de información, pieza clave de la sociedad del conocimiento, por ello, puede afirmarse que el derecho a la portabilidad de los datos es una herramienta que fomenta el libre flujo de datos. Véanse al respecto: PUCCINELLI, O.R., "El derecho a la portabilidad de los datos personales. Orígenes, sentido y alcances", *Pensamiento constitucional*, Vol. 22, Núm. 22, 2017, p. 25; STOYKOVA, R., "The right to data portability as a market tool", *Computer Law Review International*, Vol. 19, Núm. 2, 2018, p. 44

[929] GONZÁLEZ PACANOWSKA, I., "El derecho a la portabilidad de los datos personales: control y uso compartido de los datos personales" en GONZÁLEZ PACANOWSKA, I. (coord.), *Protección de datos personales*, Tirant lo Blanch, Valencia, 2020, p. 572

[930] GT29. Directrices sobre el derecho a la portabilidad de los datos, *cit.*, pp. 10-12

través de formularios en línea), pero también cuando se generan y recopilan a partir de actividades de los usuarios, mediante el uso del servicio o del dispositivo. Por el contrario, los datos personales que se deducen de los datos facilitados por el interesado, como un perfil de usuario creado por el análisis de datos en bruto por un sistema de medición inteligente, quedan excluidos del ámbito de aplicación del derecho a la portabilidad de los datos, ya que no han sido facilitados por el interesado, sino creados por el responsable del tratamiento[931].

El Considerando 68 del RGPD recoge que el derecho a la portabilidad de los datos se aplicará cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. Siguiendo con la interpretación amplia de la expresión, puede afirmarse que no solo los datos proporcionados explícitamente en un formato escrito pueden ser objeto de portabilidad, también todos los datos proporcionados sobre la base del consentimiento del interesado o dentro de la ejecución de un contrato, como cookies y datos GPS, dado que los usuarios consienten su recopilación. Sin embargo, el citado considerando, al igual que el artículo 20.3 del mismo cuerpo legal, recoge que los datos que se facilitan por motivos distintos del consentimiento o del contrato (por ejemplo, el tratamiento de datos que sea necesario para el cumplimiento de una misión realizada interés público) no pueden incluirse en el alcance de este derecho.

2.6.3. Necesidad de normas técnicas:

El artículo 20.1 del RGPD recoge que el interesado tendrá derecho a recibir sus datos personales en un formato estructurado[932], de uso común[933] y lectura mecánica[934]. Estas

[931] AEPD., "ANEXO WP242 – Preguntas más frecuentes", *aepd*, p. 2, disponible en: https://www.aepd.es/sites/default/files/2019-09/wp242rev01-annex-es.pdf

[932] El término "estructurado" significa que el software debe poder extraer elementos específicos de los datos. Los datos estructurados, tienen una configuración organizada que otorga al usuario la posibilidad de obtener resultados medibles. Esto es, los datos estructurados se administran de una manera que permite realizar consultas y generar informes, suelen ser archivos de texto que se almacenan en formato tabla, hojas de cálculo o bases de datos relacionales (las bases de datos en las que, los datos, se encuentran organizados en tablas) con títulos para cada categoría, lo que permite identificar fácilmente el dato que nos interesa. Por el contrario, los datos no estructurados necesitan herramientas analíticas más complejas para lograr este fin. Por lo tanto, se requiere intervención humana para ayudar al ordenador a leer los datos no estructurados. En el ámbito sanitario, los datos estructurados son los datos básicos del paciente (nombre, edad, sexo etc.). Por otra parte, en el grupo de los datos sanitarios no estructurados, se encuentran las radiografías, los escáneres, las TAC-s, las notas manuscritas de los médicos y las recetas hechas en papel etc. Aunque el RGPD no dice nada al respecto, se consideran formatos de archivo estructurados entre otros: CSV, EML, ICS, JSON, MBOX, TEX, VCS, XLS / XLSX y XML[932]. Véanse al respecto: WEGLARZ, G., "Two worlds of data unstructured and structured", *Information Management*, Vol. 14, Núm. 9, 2004, p. 19; WONG, J. y HENDERSON, T., "The right to data portability in practice: exploring the implications of the technologically neutral GDPR", *International Data Privacy Law*, Vol. 9, Núm. 3, 2019, p. 187

[933] Se considerará que un formato de archivo es de uso común cuando sea estructurado y de lectura mecánica sin la aplicación de otras medidas tecnologías. En otras palabras, un determinado formato será considerado de uso común cuando, su uso sea general, comprenda un alto nivel de organización y pueda ser "leído" por máquinas desde su creación, sin que para ese fin se le apliquen otras medidas tecnológicas. Asimismo, los interesados deberán tener la posibilidad de acceder a los archivos en cuestión mediante un sistema operativo popular como Linux o Windows. Véase al respecto: WONG, J. y HENDERSON, T.,

especificaciones aplicables a los medios deben garantizar la interoperabilidad del formato de los datos proporcionados por el responsable del tratamiento, siendo la interoperabilidad el resultado deseado, aunque esto no significa que los responsables del tratamiento deban mantener sistemas compatibles[935].

Según el artículo 20.2 del RGPD, el interesado tendrá derecho a que sus datos personales se transmitan directamente de un responsable a otro siempre que sea técnicamente posible. La expresión "técnicamente posible" significa que el responsable puede denegar la solicitud de portabilidad de los datos por motivos de incompatibilidad técnica con el sistema del responsable al que el interesado desea transferir sus datos. Así, si el sistema en cuestión no permite la transferencia directa de datos al responsable receptor, el responsable del tratamiento podrá denegar la solicitud. Esta condición técnica reduce significativamente la posibilidad de ejercer el derecho a la portabilidad de los datos y no impone a los responsables ninguna obligación de actualizar o modificar el sistema para que ésta sea compatible con los sistemas de otros responsables[936].

La capacidad legal de transmitir información a través de distintos servicios y plataformas es particularmente útil teniendo en cuenta la proliferación de los llamados dispositivos inteligentes. No obstante, garantizar el derecho a la portabilidad de datos en este ámbito es un desafío, puesto que, los dispositivos de IoT no solo son diversos, sino que, los proveedores, almacenan y procesan datos de manera diferente. La complejidad técnica como la falta de estándares de interoperabilidad, la escala y el alcance de los datos recopilados, así como la falta de conocimiento de los interesados sobre la naturaleza del procesamiento de datos puede dificultar la transmisión de datos entre diferentes sistemas[937]. Por tanto, debido a que la normativa de protección de datos no recoge un formato específico, fruto de la ya citada neutralidad tecnológica del RGPD, actualmente no se garantiza el ejercicio del derecho a la portabilidad de los interesados[938].

"The right to data portability in practice: exploring the implications of the technologically neutral GDPR", *cit.*, p. 187

[934] La lectura mecánica se refiere a un formato de datos que puede ser leído o descifrado por un ordenador y ser procesado automáticamente como los formatos CSV, JSON o XML. Los datos legibles por máquina deben ser datos estructurados. La portabilidad de datos puede seguir siendo inviable si los formatos de datos personales no están estandarizados. Por ello, es necesario emitir recomendaciones sobre formatos y aspectos técnicos. Véase al respecto: SOMAINI, L., "The right to data portability and user control: ambitions and limitations", *Rivista di diritto dei media*, 2018, pp. 188-189

[935] AEPD., "ANEXO WP242 – Preguntas más frecuentes", *cit*., p. 3

[936] KIVE, M. y GRASIS, J., "Problems of application of the right to data portability", *cit.*, pp. 118 y 125

[937] TURNER, S.; GALINDO QUINTERO, J.; TURNER, S.; LIS, J.; TANCZER, L.M., "The Exercisability of the Right to Data Portability in the Emerging Internet of Things (Iot) Environment", *New Media & Society*, Vol. 23, Núm.10, 2020, p. 3

[938] El derecho a la portabilidad de los datos se encuentra con un gran obstáculo en el ámbito de los dispositivos Iot: los "datos inferidos" y los "datos deducidos". Este derecho no es aplicable a los datos que se derivan del análisis de los datos facilitados por el interesado, como un perfil de usuario creado por el análisis de datos en bruto por un sistema de medición inteligente. Los usuarios pueden mover los datos personales sin procesar que alimentan estos perfiles, pero no pueden trasladar los datos procesados, siendo esto una desventaja para los mismos. Véase al respecto: URQUHART, L.; SAILAJA, N.;

2.6.4. El derecho a la portabilidad de los datos en el ámbito sanitario:

En lo relativo a la prestación de la asistencia sanitaria, el derecho a la portabilidad es uno de los derechos que cobra mayor importancia para el paciente, ya que le permite acudir a otro centro sanitario en su propio país, así como en otros países. El derecho a la portabilidad de los datos relativos a la salud no puede ejercerse en el ámbito de la salud pública, puesto que la atención sanitaria prestada por los centros y servicios de la red de salud pública no se basa ni en el consentimiento de los pacientes ni en la ejecución de un contrato. En cambio, la portabilidad de los datos sí que se puede solicitar a los responsables (mutuas privadas, médicos en ejercicio privado...) que tratan los datos de forma automatizada y de acuerdo con una decisión previa del paciente que ha contratado esta prestación[939]. Si la clínica privada está obligada a conservar los datos en el plazo estipulado por la LBAP, no los suprimirá hasta que pase dicho plazo. Por ello, la portabilidad no implica automáticamente la supresión de los datos en los sistemas informáticos del antiguo responsable[940].

Este derecho no es únicamente aplicable a nivel estatal, siendo una ventaja para la actual sociedad globalizada. Por ejemplo, si una persona se traslada de Bélgica a Alemania, puede pedir a la clínica belga a la que acudía anteriormente que le proporcione los archivos que contienen sus datos personales en un formato estructurado y de lectura mecánica para poder transmitirlos a los profesionales sanitarios de otra clínica situada en Alemania. La clínica belga deberá proporcionarle los datos personales en un formato abierto de uso común (como XML, JSON, CSV, etc.) para que el formato seleccionado no obstaculice el derecho de los pacientes[941].

En este sentido, los expertos afirman que una de las principales barreras a la hora de reconocer el derecho a la portabilidad a nivel europeo consiste en que el intercambio de datos con fines de prestación de asistencia entre distintos sistemas de salud se considera muy difícil debido a los bajos niveles de interoperabilidad entre los diversos sistemas de registros sanitarios. El derecho a la portabilidad del historial médico debería ser reconocido como obligatorio y vinculante, puesto que permite al paciente tomar decisiones en relación a su tratamiento, por ejemplo, cambiando de médico en su propio país, o solicitando asistencia en otro país de la Unión[942].

MCAULEY, D., "Realising the Right to Data Portability for the Domestic Internet of Things", *Personal and Ubiquitous Computing*, Vol. 22, Núm. 2, 2018, p. 326

[939] En este sentido, ALKORTA IDIAKEZ indica que cabe dudas de la aplicación del derecho a la portabilidad cuando los datos médicos no se recopilan sobre la base del consentimiento o del contrato, sino por necesidad de tratamiento, que es la situación más frecuente en el contexto de la prestación de asistencia sanitaria. Véase al respecto: ALKORTA IDIAKEZ, I., El espacio europeo de datos sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios, *cit.*, p. 55

[940] APDCAT. Guia de protecció de dades per a pacients i usuaris dels serveis de salud, p. 15,

[941]COMISIÓN EUROPEA. "¿Las personas pueden que sus datos se transfieran a otra organización?", *ec.europa.eu*, disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/can-individuals-ask-have-their-data-transferred-another-organisation_es *[Última consulta: 1 de agosto de 2022]*

[942] ALKORTA IDIAKEZ, I., El espacio europeo de datos sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios, *cit.*, p. 56

2.7. Derecho de oposición:

2.7.1. Concepto:

Regulado en el artículo 21 del RGPD y el artículo 18 de la LOPDGDD, el derecho de oposición permite al interesado oponerse en cualquier momento, por motivos relacionados con su situación particular, al tratamiento de sus datos personales cuando: el tratamiento de los datos personales se basa en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, pero también si el tratamiento es necesario para la satisfacción de intereses legítimos del responsable o de un tercero[943], los datos personales son tratados con fines de mercadotecnia directa[944] o cuando el tratamiento de datos personales tenga fines de investigación científica o histórica o fines estadísticos. El Tribunal Constitucional lo ha definido como la facultad de exigir a quien corresponda que ponga fin a la posesión y al uso de los datos personales[945]. No se trata de un nuevo derecho, tanto la Directiva 95/46/CE[946], como la LOPD[947] recogían el

[943] En determinadas situaciones, previa evaluación, se considerará que el tratamiento de datos es licito cuando exista un interés legítimo de un responsable o de un tercero, negándose el ejercicio del derecho de oposición. Según se indica en el Considerando 69 del RGPD, corresponderá al responsable del tratamiento la carga de la prueba.

[944] Se entiende como mercadotecnia directa cualquier acción, como el envío de correos electrónicos, que realice una empresa para enviar publicidad a particulares. Cuando el interesado ejerza su derecho de oposición, el responsable tendrá que dejar de tratar los datos personales del interesado con fines de mercadotecnia directa, incluida la elaboración de perfiles cuando la misma esté relacionada con dicha finalidad. Cuando la empresa o sociedad se dirige al cliente mediante correo electrónico, y cuando se dirige vía postal o telefónica. En el primer supuesto, son de aplicación tanto el RGPD como la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI). El artículo 21 de la LSSI prohíbe el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas, salvo cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente. La AEPD en base al RGPD y al artículo 21 de la Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI), resolvió en su Informe jurídico nº 2018-0173 de 11 de diciembre de 2018 que no se podrá enviar publicidad mediante correo electrónico si el interesado no ha otorgado el consentimiento o si no existe una relación contractual previa. En cuanto a la comunicación postal o telefónica, la AEPD en su informe jurídico de la nº 2018-0164 de 11 de diciembre de 2018 indicó que la LSSI no será de aplicación y se podrán enviar comunicaciones comerciales sin necesidad de recabar el consentimiento, en base al interés legítimo del responsable, siempre que la publicidad se refiera a productos o servicios similares contratados por el cliente**.**

[945] STC 290/2000 de 30 de noviembre de 2000 (BOE núm. 4 de 04 de enero de 2001)

[946] Considerando 45 y artículo 14 de la Directiva 95/46/CE

[947] A nivel estatal, la LOPD fue la primera normativa en incorporar el derecho de oposición, puesto que el derecho de oposición no se regulaba en la LORTAD. En el artículo 6.4 de la LOPD se recogía que en los casos en los que no fuese necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no dispusiese lo contrario, podía oponerse a su tratamiento cuando existieran motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero debía excluir del tratamiento los datos relativos al afectado. Igualmente, en el artículo 30.4 de la LOPD se recogía que los interesados tenían derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les concerniesen, siendo dados de baja del tratamiento y cancelando los datos que figurasen por su solicitud.

derecho de oposición, aunque con la entrada en vigor del RGPD y la LOPDGDD ha sufrido cambios.

Cuando el interesado ejerza su derecho de oposición, el responsable del tratamiento dejará de tratar los datos personales salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. Al no tratarse de un derecho absoluto, en algunos supuestos se deberá realizar una ponderación con el fin de considerar si prevalece o no el derecho del interesado[948]. No puede existir un derecho de oposición frente a todo, ya que en los casos de tratamientos legales, necesarios y obligatorios, la oposición al mismo no puede contemplarse, constituyendo una limitación al ejercicio del derecho[949].

2.7.2. Oposición al tratamiento de los datos relativos a la salud:

Mediante este derecho, el paciente expone su negativa a que se traten sus datos relativos a la salud. Una vez ejercido el derecho, el responsable deberá finalizar el tratamiento a menos que demuestre razones legítimas imperiosas que deben prevalecer. Este derecho puede ser limitado, si el centro sanitario puede demostrar que hay razones legítimas imperiosas que deben prevalecer, por ejemplo, si puede poner en peligro la asistencia sanitaria que recibe el paciente o el buen funcionamiento del sistema de salud[950]. La concesión del derecho de oposición no implica necesariamente la supresión de los datos, tal y como se ha indicado anteriormente, el centro puede tener la obligación de conservar la información durante un determinado periodo.

Si una autoridad de salud pública u otro organismo público, tiene un interés superior dado que está procesando datos para el bien común, por ejemplo, en una situación de pandemia, los ciudadanos pueden no tener derecho a oponerse al tratamiento de sus datos si dicho tratamiento es necesario para combatir la situación de emergencia[951].

Asimismo, el paciente podrá ejercer su derecho de oposición para el tratamiento con fines de investigación científica, histórica o para la creación de estadísticas, aunque este derecho puede ser exceptuado siempre que sea probable que se imposibilite u obstaculice gravemente el logro de los fines científico[952]. En base al artículo 21.6 del RGPD, el derecho a la oposición al tratamiento con fines de investigación científica, histórica o fines estadísticos de conformidad con el artículo 89.1 del RGPD, solo podrá

---

[948] CAMPOS ACUÑA, C., *Aplicación práctica y adaptación de la protección de datos en el ámbito local: novedades tras el reglamento europeo; el consultor de los ayuntamientos*, *cit.*, p. 153

[949] REBOLLO DELGADO, L. y SERRANO PÉREZ, M.M., *Introducción a la protección de datos*, *cit.*, p. 220

[950] APDCAT. Guia de protecció de dades per a pacients i usuaris dels serveis de salud, *cit.*, p. 16

[951] OMS., "The protection of personal data in health information systems- principles and processes for publich health", *apps.who*, 2021, p.9, disponible en: https://apps.who.int/iris/handle/10665/341374?locale-attribute=fr& *[Última consulta: 3 de agosto de 2022]*

[952] Artículo 89 del RGPD

limitarse cuando dicho tratamiento sea necesario para el cumplimiento de una misión realizada por razones de interés público. En este sentido, las excepciones a este derecho deberían estar sustentadas en la necesidad de remover un grave obstáculo para una investigación de un interés singularmente elevado[953].

2.8. Derecho a no ser objeto de decisiones individuales automatizadas:

2.8.1. Concepto:

El artículo 22 del RGPD establece que todo interesado tendrá el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Este tipo de tratamiento automatizado incluye la elaboración de perfiles[954] consistente en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar[955].

Los individuos en muchas ocasiones no son conscientes de que se están tomando decisiones que les afectan en base a esos procesos automatizados. Únicamente se toman decisiones automatizadas cuando se toman decisiones sobre la persona concreta por medios tecnológicos sin la intervención humana, incluso sin que hayan sido elaborados previamente perfiles[956]. Si un ser humano revisa y tiene en cuenta otros factores para tomar la decisión final, la misma no estará basada únicamente en el tratamiento automatizado. Para ser considerada como participación humana, el responsable del tratamiento debe garantizar que cualquier supervisión de la decisión sea significativa, en vez de ser únicamente un gesto simbólico[957].

La frase "decisión que produzca efectos jurídicos", exige que la decisión, basada únicamente en el tratamiento automatizado, afecte a los derechos jurídicos de una persona. No obstante, incluso si el proceso de toma de decisiones no afecta a sus derechos jurídicos, este aún podría ajustarse al ámbito de aplicación del artículo si

[953] NICOLÁS, P., "Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos", *Revista de Derecho y Genoma Humano*, Núm. extraordinario, 2019, p. 142

[954] En base al artículo 4.4 del RGPD se entiende por elaboración de perfiles a "*toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física*".

[955] Considerando 71 del RGPD

[956]GALINDO AYUDA, F., "¿Inteligenciaa Artificial y Derecho? Sí, pero ¿cómo?", *Revista Democracia Digital e Governo Eletrônico*, Vol.2, Núm.18, pp.53-54

[957] GT29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, *cit.*, p. 23

produce un efecto equivalente o significativamente similar en sus consecuencias. Se entiende que la decisión afecta "significativamente de modo similar", cuando impacta de un modo relevante a las circunstancias, al comportamiento o a las elecciones de las personas afectadas; tiene un impacto prolongado o permanente en el interesado o provoca la exclusión o discriminación de personas[958].

Como excepción a la prohibición, se permite el tratamiento automatizado solo cuando así lo autoriza expresamente el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento, es necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o cuando el interesado ha otorgado su consentimiento explícito. En cualquier caso, debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión[959].

Una vez expuesto el contenido del artículo 22 del RGPD, cabe preguntarse si realmente se trata de un derecho o de una prohibición. El RGPD sitúa al artículo 22 dentro de la sección 4 bajo el título de "derecho de oposición y decisiones individuales automatizadas". La LOPDGDD lo introduce en el artículo 18 relativo al derecho de oposición, aunque en su redacción separa los dos derechos. De la unión que otorga el legislador, tanto europeo como estatal, al derecho de oposición y al derecho a no ser objeto de decisiones individualizadas automatizadas, puede deducirse que esta última es la facultad que tiene el interesado a oponerse a ser objeto de una decisión basada únicamente en el tratamiento automatizado, pudiendo entenderse que se trata de un derecho del interesado. Por su parte, la AEPD al definirlo utiliza la frase "este derecho pretende garantizar", refiriéndose a él como derecho, y poniendo a disposición del interesado el modelo para su ejercicio en su página web[960].

En sentido contrario, el GT29 ha manifestado que se trata de una prohibición, no de un derecho[961]. A su vez, el Tribunal de la Haya en su sentencia de 5 de febrero de 2020 indicó que en virtud del artículo 22 del RGPD existe una prohibición general de tomar decisiones individuales automatizadas, incluida la elaboración de perfiles, que produzcan efectos jurídicos en el interesado o le afecten significativamente de modo similar, aunque existen excepciones[962]. En consecuencia, se podría interpretar que es una prohibición automática, aunque se identifican excepciones o bases legitimadoras para poder llevar a cabo la toma de decisiones individuales automatizadas.

---

[958] Ibid., p. 22

[959] Considerando 71 y artículo 22.2 del RGPD

[960] AEPD., "Derecho a no ser objeto de decisiones individuales automatizadas", *aepd*, 14 de junio de 2022, disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-no-ser-objeto-de-decisiones-individuales *[Última consulta: 7 de agosto de 2022]*

[961] GT29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, *cit.*, p. 22

[962] Sentencia del Tribunal de la Haya C/09/550982 / HA ZA 18-388 de 5 de febrero de 2020, (ECLI: NL: RBDHA: 2020: 865) párrafo 6.35

Este razonamiento gana peso si se analizan los artículos 13.2.f), 14.2.g) y 15.1.h) del RGPD, puesto que los mismos establecen que el interesado ha de ser informado sobre la existencia de la toma de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22 del RGPD. Por ello, existirá una obligación de informar al interesado cuando la toma de decisiones automatizada está legitimada por el Derecho de la Unión o de los Estados miembros, por ser necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o cuando el interesado ha otorgado su consentimiento explícito, lo cual exceptuará la prohibición general. Todo lo expuesto hace defendible la idea de que el artículo 22 del RGPD realmente se refiera a una prohibición y no a un derecho, pero su ambigua redacción sigue generando dudas[963].

2.8.2. El derecho a no ser objeto de decisiones individuales automatizadas en el ámbito sanitario:

El ámbito sanitario es uno de los escenarios en los que puede darse el fenómeno de la toma de decisiones individualizadas automatizadas. Como ya se ha puesto de manifiesto en el capítulo primero del presente trabajo, la aplicación de algoritmos a los datos relativos a la salud puede tener como resultado la adopción de medidas que discriminen o incluso pongan en peligro la salud del interesado. Por ejemplo, piénsese en el caso de la aplicación de algoritmos a los datos recolectados mediante la monitorización que se está realizando se deduce que una persona tiene una determinada enfermedad sin que un médico intervenga, puede aplicarse un tratamiento médico no adecuado que perjudique la salud del paciente. Actualmente, también la investigación básica con intervención física sobre el paciente o voluntario está siendo sustituida en parte por la investigación con datos sometidos a fórmulas algorítmicas.

El uso de la inteligencia artificial para el diagnóstico o la investigación puede poner de relieve una realidad oculta entre la multitud de los datos del interesado, permitiendo, entre otras cuestiones, una temprana detección de enfermedades. A pesar de los potenciales beneficios de su uso, no es menos cierto que también pueden realizar erróneas deducciones, de ahí la necesidad de un control humano. Las personas tenemos la capacidad de apreciar determinados elementos intangibles que no son captados por los sistemas automatizados, por ello, existe una alta probabilidad de que se produzcan errores o se introduzcan sesgos durante el desarrollo de los sistemas algorítmicos e incluso tras su puesta en funcionamiento. Es por ello que esa "mayor objetividad" de los algoritmos ha de ser cuestionado y deben diseñarse e implementarse mecanismos de control jurídico e informático que traten de prevenir y lidiar con los errores y sesgos producidos por los procesos de toma de decisiones automatizadas[964].

[963] En el mismo sentido: WACHTER, S.; MITTELSTADT, B.; FLORIDI, L., "Why a right to explanation of automated decision-making does not exist in the general data protection regulation", *International Data Privacy Law*, Vol. 7, Núm. 2, 2017, p.98

[964] SORIANO ARNANZ, A., "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos", *Revista de derecho público: teoría y método*, Vol. 3, 2021, pp. 90-91

Por esta razón, el artículo 22.4 del RGPD opera una mayor restricción en ciertos ámbitos entre los que se identifica el sanitario, puesto que solo se permite la adopción de decisiones basadas únicamente en tratamientos automatizados con datos que pertenezcan a las categorías especiales de datos personales, cuando sea de aplicación el artículo 9.2.a) o el artículo 9.2.g) del RGPD y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado. Esto es, cuando el interesado haya otorgado su consentimiento explícito o el tratamiento es necesario por razones de un interés público esencial.

3. EL EJERCICIO DE LOS DERECHOS POR PARTE DE LA PERSONA MAYOR CON DISCAPACIDAD:

3.1. Legitimidad y solicitud:

De acuerdo con la doctrina clásica sobre los derechos de la personalidad, también el derecho fundamental a la protección de datos personales como tal sería un derecho personalísimo, lo cual conlleva que deba ser ejercitado por el propio interesado tras identificarse adecuadamente.

En el caso de menores de catorce años, la LOODGDD establece que estarán legitimados para presentar las solicitudes quienes tengan su patria potestad[965]. En el supuesto citado, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años sus derechos ARSLOP[966]. La AEPD, ha declarado que el ejercicio de los menores no puede entenderse como limitación al derecho de los titulares de la patria potestad del menor no emancipado a acceder a su historia clínica y el menor no puede impedirlo. Por lo tanto, el menor no emancipado no puede oponerse al acceso de sus padres a la información clínica. La habilitación para acceder al historial clínico se refiere solo a los titulares de la patria potestad y no a cualesquiera familiares. Los titulares de la patria potestad tienen derecho a acceder a la historia clínica de los menores que tengan a su cargo en base a su obligación de velar por su salud y bienestar,

[965] En ámbito sanitario, en el caso de los menores de edad se da una especialidad. Por una parte, el artículo 9.4 de la LBAP recoge que los mayores de 16 años o menores emancipados podrán otorgar su consentimiento informado, no cabiendo prestar el consentimiento por representación. El artículo 8.1 del RGPD sigue esta línea al exponer que si el niño es menor de 16 años, el tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. No obstante, el mismo artículo dice que los estados miembros podrán establecer por ley una edad inferior a tales fines. Así, en el artículo 7.1 de la LOPDGDD se pone el límite en los 14 años. El artículo 12.4 del Decreto 38/2012 recoge que en el caso de los pacientes menores de 16 años de edad, sin emancipación, el ejercicio del derecho de acceso a su historia clínica requerirá contar en todo caso con la autorización expresa de sus progenitores o de sus representantes legales, no estando legitimados para acceder a la historia clínica los menores de 16 años.
Por ello, puede decirse que existe una contradicción entre la normativa de protección de datos y la normativa sanitaria.

[966] Artículo 12 de la LOPDGDD

siendo necesario que conozcan los datos relativos de salud que se encuentran recogidos en la historia clínica[967].

Por otra parte, tras la entrada en vigor de la Ley 8/2021 analizada previamente, y tal y como se ha indicado en el capítulo tercero, se ha de realizar una interpretación del artículo 12.1 de la LOPDGDD acorde a la reforma, entendiendo que las personas mayores con discapacidad serán quienes ejerzan estos derechos con el apoyo que requieran. En los casos más extremos donde sea necesario un apoyo con funciones de representación porque la persona no pueda expresar su voluntad, la persona encargada de apoyarla deberá averiguar su voluntad, deseos y preferencias. Para garantizar que se respete esta voluntad, lo más adecuado sería que la persona interesada haya indicado anteriormente en escritura pública que el apoyo que necesite también se otorgue en el ámbito de protección de datos, delimitando el régimen de actuación de la persona que le prestará el apoyo e introduciendo un listado que refleje su voluntad deseos y preferencias que deberá respetar la persona encargada de otorgar el apoyo. Cuando el derecho sea ejercido mediante un apoyo, se deberá indicar el nombre, apellido y número de identificación de este tercero junto con los datos del interesado, adjuntando, en su caso, copia del poder o de la resolución de la medida de apoyo judicial. Veamos a continuación, cuál será la forma en la que el interesado con discapacidad puede ejercitar cada uno de los derechos mencionados en el apartado anterior.

Para el ejercicio del derecho de acceso[968], el interesado, con el apoyo que necesite, se deberá dirigir directamente al responsable del tratamiento y este deberá adoptar medidas para que sea un acceso seguro de manera que, entre otras cuestiones, se eviten riesgos de acceso no autorizados por terceros[969]. En el ámbito sanitario, el interesado tiene que dirigirse directamente a la persona responsable del centro o servicio sanitario o, en su caso, al servicio correspondiente de atención a pacientes, especificando la información que solicita y de qué episodio asistencial se trata[970].

Respecto a la solicitud de rectificación[971], no basta con la simple manifestación de voluntad del titular de los datos personales para lograr el cambio de sus datos. Además de la solicitud, el interesado, valiéndose del apoyo que necesite, debe adjuntar pruebas que pongan de manifiesto que sus datos, en el presente caso, datos relativos a la salud, no son correctos o que son incompletos[972]. El solicitante del derecho debe dirigirse

[967] AEPD. ,"¿Pueden acceder los padres a las historias clínicas de sus hijos mayores de 14 años?", *aepd*, disponible en: https://www.aepd.es/es/preguntas-frecuentes/10-menores-y-educacion/FAQ-1005-pueden-acceder-los-padres-a-las-historias-clinicas-de-sus-hijos-mayores-de-14 *[Última consulta: 10 de agosto de 2022]*

[968] AEPD., "Formulario del derecho de acceso", *aepd*, disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-acceso.pdf

[969] Considerando 63 del RGPD: *"el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales".*

[970] Artículo 12.5 del Decreto 38/2012

[971] AEPD., "Formulario del derecho de rectificación", *aepd*, disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-rectificacion.pdf

[972] Artículo 27.1 del Decreto 38/2012

directamente al órgano del que presume o tiene la certeza de que posee sus datos[973]. En cuanto al ejercicio del derecho de supresión y al olvido, el interesado, debidamente apoyado, deberá dirigirse directamente ante el organismo público o privado, empresa o profesional del que presume o tiene la certeza que posee sus datos[974].

En la solicitud relativa a la limitación del tratamiento, el interesado, con el apoyo que necesite, deberá especificar qué condición se da. Es decir, si el tratamiento es ilícito y se opone a la supresión o si el responsable ya no necesita sus datos personales para los fines para los cuales fueron recabados, pero el interesado los necesita para la formulación, ejercicio o defensa de sus reclamaciones[975]. Con el objetivo de acreditar los motivos de limitación del tratamiento, el interesado deberá aportar la documentación oportuna.

Para la solicitud de la portabilidad de los datos, el interesado, con el apoyo que necesite, deberá solicitar que se le faciliten sus datos personales en un formato estructurado, de uso común y lectura mecánica. En su caso, siempre que sea técnicamente posible, el interesado podrá solicitar que los citados datos personales sean transmitidos directamente al nuevo responsable, especificando nombre o razón social[976].

Para llevar a cabo la solicitud de oposición el interesado, el interesado con discapacidad debidamente apoyado, deberá especificar qué condición se da: si el tratamiento de sus datos personales se basa en una misión de interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, si el tratamiento de sus datos personales se basa en la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o un tercero o si el tratamiento de sus datos personales se está realizando con fines de investigación científica o histórica o fines estadísticos[977]. Igualmente, y sin perjuicio de que corresponde al responsable del tratamiento acreditar motivos legítimos imperiosos que prevalezcan sobre mis intereses, derechos y libertades en los dos primeros supuestos, o una misión realizada en interés público en el tercer supuesto, el interesado deberá exponer cuáles son sus motivos personales para oponerse al tratamiento de sus datos personales[978].

Por último, la AEPD también ha creado un modelo para el ejercicio del derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que le produzcan al interesado efectos jurídicos o le afecten

---

[973] AVPD., "Mis derechos", *avpd,* disponible en: https://www.avpd.euskadi.eus/s04-5273/es/contenidos/informacion/misderechos/es_def/index.shtml#10 *[Última consulta: 14 de agosto de 2022]*

[974] AEPD., "Formulario del derecho de supresión", *aepd,* disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-supresion.pdf

[975] AEPD., "Formulario del derecho de limitación del tratamiento", *aepd,* disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-limitacion.pdf

[976] AEPD., "Formulario del derecho de la portabilidad", *aepd,* disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-portabilidad.pdf

[977] AEPD., "Formulario del derecho de oposición", *aepd,* disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-oposicion.pdf

[978] Artículo 27.3 del Decreto 38/2012

significativamente de modo similar. En particular, junto con la adopción de medidas necesarias para salvaguardar sus derechos y libertades, el interesado, con el apoyo que necesite, solicitará la intervención humana[979].

Tal y como se ha indicado previamente, cuando cualquier derecho del interesado sea ejercido con el apoyo de una tercera persona, se deberá indicar el nombre, apellido y número de identificación de este tercero junto con los datos del interesado, adjuntando, en su caso, copia del poder o de la resolución de la medida de apoyo judicial. Sin embargo, en los formularios que proporcionan tanto la AEPD como la AVPD en sus respectivas páginas oficiales se sigue manteniendo el apartado de los "datos del representante legal", el cual, en relación con la reforma operada por la Ley 8/2021 debe ser modificado por "datos de la persona que otorga el apoyo para el ejercicio de los derechos al interesado", con el fin de recoger el caso de las personas con discapacidad.

En los casos en los que no se acepte la solicitud del interesado, resultará necesario realizar una correcta ponderación de los derechos e intereses en conflicto, atendiendo a las circunstancias concurrentes en el caso concreto. Cuando proceda el ejercicio de dichos derechos, el mismo no tendrá coste alguno. En el caso de que las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, se podrá cobrar un precio razonable o negarse a actuar respecto a la solicitud, pudiendo aplicar al solicitante un canon por los costes administrativos acarreados[980]. Se podrá considerar que una solicitud es repetitiva cuando se haya ejercido en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello. Una solicitud será considerada excesiva cuando el afectado elija un medio distinto al que se le ofrece y este hecho suponga un coste desproporcionado[981].

Las solicitudes deben responderse en el plazo de un mes, aunque, aunque si la solicitud es compleja o existen numerosas solicitudes, se puede prorrogar el plazo otros dos meses. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Si la solicitud se presenta por medios electrónicos, la información se facilitará, cuando sea posible, de la misma manera salvo que el interesado solicite que sea de otro modo. Es decir, si la solicitud se ha hecho a través de medios digitales, se deberá atender por el mismo medio, salvo que el interesado decida ser atendido por otro canal[982]. Si el responsable no da curso a la solicitud, informará en el plazo máximo de en un mes de las razones de su no actuación y la posibilidad de que el interesado pueda reclamar ante una Autoridad de Control[983].

---

[979] AEPD., "Formulario del derecho a no ser objeto de decisiones individuales automatizadas", *aepd*, disponible en: https://www.aepd.es/es/documento/formulario-derecho-de-oposicion-decisiones-automatizadas.pdf

[980] Artículo 12.5 del RGPD

[981] AEPD. Resolución R/00253/2022 de 10 de junio de 2022 (expediente núm: EXP202101463)

[982] Artículo 12.3 del RGPD

[983] Artículo 12.4 del RGPD

3.2. Tutela de los derechos del interesado:

El interesado que considere que se han lesionado sus derechos en materia de protección de datos, podrá reclamar directamente ante el DPO o iniciar el procedimiento ante la AEPD o, también, ante las agencias autonómicas de protección de datos. Por su parte, las actuaciones contrarias a lo dispuesto en la LOPDGDD pueden ser objeto de reclamación por los interesados ante la AEPD o, en su caso, ante las autoridades autonómicas de protección de datos, puesto que su función es la de velar por el cumplimiento de la legislación y controlar su aplicación. Por esta razón, la AEPD y las autoridades autonómicas de protección de datos disponen de la potestad de inspección y sanción de las infracciones que constate. Contra estas últimas resoluciones procederá recurso contencioso-administrativo[984].

En el primer supuesto, en el caso de que el responsable o el encargado del tratamiento hubieran designado un DPO, el interesado, con el apoyo que requiera, podrá con carácter previo a la presentación de una reclamación ante la AEPD o, en su caso, ante la autoridad autonómica de protección de datos**,** dirigirse al DPO de la entidad contra la que reclame. Este último deberá comunicar al interesado la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación[985].

El interesado, con el apoyo que necesite, tendrá la opción de acudir directamente ante la AEPD o ante la autoridad autonómica de protección de datos, comenzando un procedimiento de tutela de derechos. Una vez recibida la reclamación, la AEPD o la autoridad autonómica de protección de datos, tendrá la posibilidad de remitir la reclamación al DPO o al organismo que se haya establecido para la supervisión de los códigos de conducta. En el caso de que no se haya designado un DPO o no se hubiera adherido al Código de Conducta de la entidad, se podrá remitir la reclamación al responsable o encargado[986].

En base al artículo 65 de la LOPDGDD, la autoridad de protección de datos evaluará la admisibilidad de la reclamación, inadmitiendo cuando no versen sobre protección de datos, carezcan manifiestamente de fundamento, sean abusivas o no aporten indicios racionales de la existencia de una infracción. Se contempla también la inadmisión en el caso de que la AEPD hubiera advertido previamente al responsable o encargado del tratamiento de las medidas encaminadas para poner fin al incumplimiento, siempre y cuando se traten de infracciones leves y no se haya perjudicado al afectado o cuando el derecho del afectado quede plenamente garantizado mediante la aplicación de las medidas. La autoridad de control deberá notificar al reclamante en el plazo de tres meses su decisión sobre la admisión o inadmisión a trámite de la reclamación, si no se contesta en ese plazo se entiende que prosigue la tramitación de la reclamación y la

[984] PÉREZ RODRÍGUEZ, M.D., *Ley de Protección de datos,* ICB, Madrid, 2017, p. 88
[985] Artículo 37.1 de la LOPDGDD
[986] Artículos 37.2 y 65.4 de la LOPDGDD

autoridad de protección de datos otorgará una resolución que resuelve la reclamación del interesado. El incumplimiento de esa resolución podría comportar la comisión de una infracción recogida en el artículo 83.5 del RGPD.

En cuanto al procedimiento sancionador, este se divide en tres fases (iniciación, instrucción y resolución) en las que se integran las diferentes actuaciones administrativas, intentando garantizar la transparencia, la contradicción y la oportunidad de resolución. Con anterioridad a la estricta tramitación del procedimiento, existen dos fases previas: admisión a trámite de la reclamación y actuaciones previas al inicio del expediente[987]. Si la AEPD o la autoridad autonómica de protección de datos considera que se ha cometido una infracción podrá sancionar con multas administrativas de 20.000.000€ como máximo o, tratándose de empresas, de una cuantía equivalente al 4% como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía[988]. Sin embargo, si la infracción ha sido cometida por un organismo público la autoridad de protección de datos que resulte competente sancionará al mismo con apercibimiento, actuaciones disciplinarias, amonestación y publicación en el Boletín Oficial del Estado o autonómico que corresponda[989].

El artículo 83.7 del RGPD contempla la posibilidad de que cada Estado miembro pueda establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro. No obstante, la LOPDGDD no contempla las multas económicas para determinadas categorías de responsables o encargados del tratamiento entre las que se incluyen los organismos públicos. Esta apuesta por parte del legislador estatal puede ser muy criticable, puesto que, refleja la inmunidad de los organismos públicos en materia de protección de datos personales.

A modo ejemplificativo, el paciente mayor con discapacidad al que se le haya privado el derecho de acceso a la historia clínica tendrá dos vías para reclamar su derecho. Si el interesado, debidamente apoyado, acude al DPO, este deberá comunicarle la decisión que se hubiera adoptado en el plazo máximo de dos meses a contar desde la recepción de la reclamación[990]. Si por el contrario acude a la AEPD o a la autoridad autonómica de protección de datos, una vez recibida la reclamación, tendrá la posibilidad de remitir la reclamación al DPO del centro sanitario. El DPO, contará con un mes para justificar la actuación del centro ante la solicitud del paciente. La autoridad de protección de datos competente evaluará la admisibilidad de la reclamación y notificará al reclamante en el plazo de tres meses su decisión sobre la admisión o inadmisión a trámite de la reclamación, si no se contesta en ese plazo se entiende que prosigue la tramitación de la

[987] APARICIO SALOM, J. y VIDAL LASO, M., Estudio sobre la protección de datos, cit., p. 405
[988] Artículo 83.5.b) del RGPD
[989] Artículos 50, 77.2 y 77.3 de la LOPDGDD
[990] Artículo 37.1 de la LOPDGDD

reclamación. Finalmente, se otorgará una resolución que resuelve la reclamación del interesado.

Cuando la resolución de la autoridad de protección de datos competente inste al organismo reclamado a facilitar el acceso a su historia clínica al interesado, pero el organismo en cuestión no lo lleva a cabo, se podrá dar comienzo a un procedimiento sancionador. Si al finalizar el procedimiento sancionador la AEPD o, en su caso, la autoridad autonómica de protección de datos considera que se ha infringido el derecho de acceso del interesado, la sanción dependerá de si el centro sanitario infractor es público o privado. Cuando se trate de un centro público, podrá ser sancionado con apercibimiento, actuaciones disciplinarias, amonestación y publicación en el Boletín Oficial del Estado o autonómico que corresponda, pero no con una sanción económica. Sin embargo, cuando el centro sea privado, se le impondrá una multa económica aun habiendo infringido el mismo derecho del interesado.

4. EL EJERCICIO DE LOS DERECHOS DE PROTECCIÓN DE DATOS EN EL ÁMBITO SANITARIO TRAS EL FALLECIMIENTO DEL INTERESADO:

Como es sabido, la normativa de protección de datos no es de aplicación a los tratamientos de datos personales de personas fallecidas[991]. Esta exclusión se basa en el artículo 32 del CC, el cual establece que el fallecimiento de una persona determina la extinción de su personalidad civil. El Tribunal Constitucional, por su parte, afirmó que, *si el derecho fundamental a la protección de datos ha de ser considerado como el derecho del individuo a decidir sobre la posibilidad de que un tercero pueda conocer y tratar la información que le es propia, dicho derecho desaparece por la muerte de las personas, porque los tratamientos de datos personas fallecidas no podrían considerarse comprendidos dentro del ámbito de aplicación de la Ley*[992].

Aunque el RGPD establezca que la normativa de protección de datos no es de aplicación a los tratamientos de datos personales de personas fallecidas, los Estados miembros son competentes para establecer normas relativas al tratamiento de los datos personales de estas.

Esto significa que el legislador europeo ha renunciado a armonizar la regulación sobre el tratamiento de los datos de las personas fallecidas. Una de las razones de dicha elección puede ser la gran diversidad de los sistemas de Derecho sucesorio que coexisten en los Estados miembros y su gran arraigo con la tradición jurídica nacional[993].

[991] Considerando 27, 158 y 160 del RGPD y artículo 2.b) de la LOPDGDD
[992] STC 292/2000 de 30 de noviembre de 2000 (BOE núm. 4 de 4 de enero de 2000)
[993] DÍAZ ALABART, S., *La protección de los datos y contenidos digitales de las personas fallecidas*, Reus, 2021, p. 23

En el caso español, el artículo 2.2 de la LOPDGDD dice que esta ley orgánica no es aplicable a los tratamientos de datos de personas fallecidas[994]. No obstante, la LOPDGDD regula tanto el acceso a los datos personales del fallecido como el acceso a contenidos del fallecido que están gestionados por prestadores de servicios de la sociedad de la información en los artículos 3 y 96 de la LOPDGDD respectivamente. El artículo 3 de la LOPDGDD regula el acceso a los datos personales del fallecido, y el artículo 96 de la LOPDGDD se refiere al acceso *post mortem* de cualquier contenido en formato digital de la persona fallecida. Al tratarse de accesos tan distintos, es necesaria una labor interpretativa para comprender el alcance de cada artículo.

En primer lugar se examinará el título de "datos de las personas fallecidas". En el artículo 3 de la LOPDGDD se dice que las personas vinculadas a la persona fallecida por razones familiares o de hecho así como sus herederos podrán dirigirse al responsable o encargado del tratamiento para solicitar el acceso a los datos personales de aquella, y en su caso, su rectificación o supresión, siempre que la persona fallecida no lo hubiese prohibido expresamente o así lo establezca una ley. La LOPDGDD parte de la regla de acceso, y esta solo se prohíbe por la negativa del fallecido o cuando lo establezca la ley. Como critica, podría afirmarse que legitimar, salvo prohibición expresa por parte del fallecido o de una ley, a las personas que simplemente tengan un vínculo con la persona fallecida por razones familiares o de hecho es excesivo. A su vez, el citado artículo no determina cuál es el grado de parentesco que se ha de cumplir, si las razones de hecho solo se refieren a las parejas de hecho ni si estas han de estar registradas.

En base al artículo 3.3 de la LOPDGDD, las personas o instituciones a las que el fallecido hubiese designado expresamente para ello podrán también solicitar, con arreglo a las instrucciones recibidas, el acceso a los datos personales de este y, en su caso su rectificación o supresión. En caso de fallecimiento de personas con discapacidad, estas facultades también podrán ejercerse por quienes hubiesen sido designados para el ejercicio de funciones de apoyo, si tales facultades se entendieran comprendidas en las medidas de apoyo prestadas por el designado. Este apartado es realmente curioso, puesto que habla de medidas de apoyo aun cuando a la hora de su redacción quedaban tres años para la entrada en vigor de la Ley 8/2021. Cuando se hayan establecido medidas de apoyo voluntarias que recojan la actuación del prestador de apoyo en el ámbito de protección de datos personales, tras el fallecimiento del interesado, el prestador de apoyo podrá ejercer estas facultades. Cuando se hayan

[994] Según afirma NICÓLAS JIMENEZ, la exclusión de los datos de fallecidos del ámbito de aplicación del RGPD y de la LOPDGDD no significa que su procesamiento para investigación no deba estar sujeto a ciertas garantías previstas en la legislación específica. Así, se exige evaluación de un CEI para la utilización de muestras biológicas de fallecidos con fines de investigación (art. 62 LIB y 26.2 RD 1716/2011), y este requisito debería también aplicarse al supuesto de uso de datos. Véase al respecto: NICOLÁS JIMÉNEZ, P., y TERRIBAS I SALA, N., "Investigación con datos de carácter personal", en ROMEO CASABONA, C.M (Dir.); NICOLÁS JIMÉNEZ, P., y ROMEO MALANDA, S. (Coord.), *Manual de bioderecho (Adaptado para la docencia en ciencias de la salud y ciencias sociales y jurídicas), cit.*, p. 698

establecido medidas judiciales, la persona que otorgaba el apoyo al interesado podrá ejercer los derechos del interesado siempre que en las medidas de apoyo judiciales se comprendieran estas facultades. El problema interpretativo surge cuando la medida de apoyo fuese de carácter informal, no obstante, como el guardador de hecho generalmente es un familiar del interesado, este caso podría entrar dentro del apartado 1 del artículo 3 de la LOPDGDD "las personas vinculadas al fallecido por razones familiares o de hecho".

En virtud del artículo 12.5 del RGPD, cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos, se estará a lo dispuesto en aquellas. Respecto al ámbito sanitario, el artículo 18.4 de la LBAP establece que los centros sanitarios y los facultativos de ejercicio individual solo facilitarán el acceso a la historia clínica del paciente fallecido a las personas vinculadas a él por razones familiares o de hecho, salvo que el fallecido lo hubiese prohibido expresamente y así se acredite. En cualquier caso, el acceso de un tercero a la historia clínica motivado por un riesgo para su salud se limitará a los datos pertinentes, no se facilitará información que afecte a la intimidad del fallecido ni a las anotaciones subjetivas de los profesionales, ni que perjudique a terceros[995].

El artículo 14.3 del Decreto 38/2012 establece que se podrá producir el acceso a la documentación de la historia clínica de las personas fallecidas por terceras personas que acrediten su vinculación con aquéllas por razones familiares o de hecho[996], siempre que se justifiquen motivos por un riesgo para la propia salud de la persona solicitante y salvo que la persona fallecida lo hubiese prohibido expresamente y así se acredite. En todo caso, el acceso se limitará a los datos pertinentes y no se facilitará información que afecte a la intimidad de la persona fallecida, ni a las anotaciones subjetivas de los y las profesionales que intervinieron, ni que perjudique a terceras personas. La legitimación automática que otorgan la LBAP y el Decreto 38/2012 a los familiares del fallecido puede considerarse excesiva. Por ejemplo, en el caso de que la hija de una persona fallecida por una determinada enfermedad comenzase con los mismos síntomas que la difunta, es defendible que pueda solicitar el acceso a parte del historial clínico, siempre limitado a lo necesario, de su fallecida madre para comprobar si se trata de una enfermedad hereditaria en base a un interés propio que se traduciría en la temprana detección de la enfermedad, pero no por el simple hecho de ser su hija. Por ello, sería más adecuado que las bases legitimadoras fusen la justificación de un interés propio o la designación expresa del fallecido.

Cabe preguntarse quienes son realmente las personas legitimadas, es decir, los familiares de qué grado podrán solicitar el acceso y en su caso rectificación y supresión de los datos relativos a la salud del historial clínico del fallecido. Pues bien, ni el LBAP ni el Decreto 38/2012 definen el grado de parentesco, y tampoco precisan si las parejas

[995] Resolución de la AEPD R/01237/2018 de 5 de julio de 2018 (Procedimiento núm: TD/00685/2018) y el dictamen de la APDCAT CNS 8/2019 de 18 de febrero de 2019
[996] AVPD. Dictamen D09-051 de 26 de octubre de 2009 (Expediente CN09-044)

de hecho han de estar inscritas en el registro de parejas o si es suficiente con acreditar la convivencia. Según TRONCOSO REIGADA, la consideración de familiar debe alcanzar al cónyuge, hijos, padres y hermanos, y la relación de hecho debe estar acreditada en el correspondiente registro o con la inscripción en el padrón municipal. En cuanto a los terceros, según el autor, son aquellas personas que no están vinculadas al paciente por razones familiares o de hecho, y solo pueden acceder a la historia clínica cuando exista un grave riesgo para su salud y no a toda ella, sino solo a los datos pertinentes[997].

Por su parte, la AEPD en su Informe 171/2008 de 4 de agosto de 2008 indica que el ejercicio del derecho de acceso a la historia clínica del fallecido corresponde a su cónyuge o persona vinculada con aquél por una relación de hecho similar, a los ascendientes y a los descendientes. En cuanto a los hermanos, la AEPD no los menciona, sin embargo, podría interpretarse que se trata un error, puesto que el texto se basa en el artículo 4 de la Ley Orgánica 1/1982, de 5 de mayo, reguladora de la protección civil de los derechos fundamentales al honor, a la intimidad personal y familiar y a la propia imagen, la cual sí que los contempla entre los legitimados.

En el caso del artículo 14.3 del Decreto 38/2012, su confusa redacción puede crear problemas interpretativos. De la frase "terceras personas que acrediten su vinculación con aquéllas por razones familiares o de hecho", se puede deducir que las terceras personas serán aquellas que tengan una relación familiar o de hecho directa con el fallecido. Seguidamente, el artículo en cuestión indica que este acceso se permitirá "siempre que se justifiquen motivos por un riesgo para la propia salud de la persona solicitante". En consecuencia, podría comprenderse que la normativa solo permite el acceso a la historia clínica del fallecido a aquellas terceras personas que acrediten su relación familiar o de hecho con el difunto y justifiquen un motivo de riesgo para su salud, debiendo cumplirse las dos condiciones.

No obstante, la AVPD en su dictamen de 30 de mayo de 2019[998] ha concluido que estarán legitimados para acceder a la historia clínica del fallecido, salvo oposición expresa del mismo debidamente acreditada, su cónyuge o pareja de hecho, ascendientes, descendientes y hermanos. Quienes no acrediten ese parentesco o el vínculo de hecho, serán considerados como terceros, y al igual que los familiares afectados por la oposición expresa del fallecido, únicamente accederán a la historia clínica de este cuando exista un riesgo para su salud, y exclusivamente a aquellos datos clínicos del difunto estrictamente necesarios para proteger ese bien jurídico, salvo que fuesen designados en el testamento para el ejercicio de las acciones de la LO 1/1982, o herederos. Según la interpretación de la AVPD, las personas que acrediten una relación familiar o de hecho del difunto estarán siempre legitimadas para acceder a la historia clínica del fallecido salvo que este lo hubiese prohibido. En este último caso, al igual

[997] TRONCOSO REIGADA, A., *La protección de datos personales: en busca del equilibrio*, Tirant lo Blanch, Valencia, 2010, pp. 1196-1197

[998] AVPD. Dictamen D19-008 de 30 de mayo de 2019 (Expediente CN19-003)

que ocurre con las terceras personas, solo podrán acceder a la historia clínica de la persona fallecida si existe un riesgo para su propia salud, debiendo delimitarse el acceso a los datos clínicos necesarios.

En esta misma línea, en la recomendación realizada por el Defensor del Pueblo[999] al servicio vasco de salud (Osakidetza), se recoge que las peticiones de acceso de familiares de personas fallecidas se deben resolver previa comprobación de su condición de familiares y de la inexistencia de una prohibición expresa de la persona fallecida para ese acceso, y la falta de acreditación de justificación de un riesgo para la propia salud de la persona solicitante no puede ser interpretada como causa de denegación en estos procedimientos de acceso[1000].

En cuanto al segundo tipo de acceso, bajo el título de "derecho al testamento digital", el artículo 96 de la LOPDGDD regula el acceso a contenidos gestionados por prestadores de servicios de la sociedad de la información sobre personas fallecidas. Debido al uso de las palabras "testamento" y "digital", se podría llegar a interpretar erróneamente que el legislador se refiere al formato utilizado para realizar el acto jurídico, siendo necesario diferenciarlo del testamento online. En el testamento digital se recoge la voluntad de una persona sobre su contenido digital para el caso en que fallezca, y el testamento online es el testamento que se realiza en línea, formato que no se contempla expresamente en el CC aunque existan empresas que lo ofrecen[1001].

El artículo 96 de la LOPDGDD se refiere a la gestión de los contenidos digitales tras el fallecimiento del interesado[1002]. Estos contenidos digitales no solo son bienes en su sentido clásico, la huella que deja la actividad del interesado en la red puede tener tanto carácter patrimonial como no patrimonial. A pesar de que no exista una descripción en la LOPDGDD, el término contenido digital se puede utilizar para describir sitios web, dominios, criptomonedas[1003], cuentas electrónicas (banca online o servicios de pago), cuentas de correo electrónico o cuentas de redes sociales[1004]. Aunque las cuentas sean catalogadas dentro de la definición de contenido digital, en realidad son relaciones obligatorias de naturaleza contractual en cuya virtud un prestador de servicios de

[999] Defensoría del pueblos del País Vasco
[1000] ARARTEKO. Recomendación general 9/2013 de 5 de noviembre
[1001] LLOPIS BENLLOCH ha manifestado que el testamento online no existe en la realidad. Véase al respecto: LLOPIS BENLLOCH, J.C., "Con la muerte digital no se juega: el testamento online no existe", en OLIVA LEÓN, R. y VALERO BARCELÓ, S., *Testamento ¿Digital?*, Colección Desafíos legales, Juristas con futuro, 2016, p. 49
[1002] MARTÍNEZ MARTÍNEZ, N., "Reflexiones en torno a la protección post mortem de los datos personales y la gestión de la transmisión mortis causa del patrimonio digital tras la aprobación de la LOPDGDD", *Derecho Privado y Constitución*, Núm. 35, 2019, pp 178 y 207
[1003] En la STS Sala de lo Penal 326/2019, de 20 de junio de 2020 (Rec. Núm. 998/2018) se afirmó que el "*bitcoin no es sino un activo patrimonial inmaterial, en forma de unidad de cuenta definida mediante la tecnología informática y criptográfica denominada bitcoin, cuyo valor es el que cada unidad de cuenta o su porción alcance por el concierto de la oferta y la demanda en la venta que de estas unidades se realiza a través de las plataformas de trading Bitcoin*".
[1004] CONNER, J., "Digital life after death: The issue of planning for a person's digital assets after death", Texas Tech Law School Research Paper, Núm. 10, 2010, p. 548

internet ofrece al usuario determinados servicios de carácter digital. A su vez, es posible que exista una intransmisibilidad establecida en el contrato celebrado por el usuario y el prestador de servicios cuando el causante no tuviese un derecho de propiedad sino una licencia de uso sobre el bien, por ejemplo, música, videos o libros digitales[1005].

En cuanto a los archivos, la norma alude exclusivamente a aquellos contenidos digitales que estén siendo gestionados por prestadores de servicios de la sociedad de la información, por lo que se entiende que los archivos deben de estar en la nube, no en un soporte físico como el disco duro del ordenador o en un *pen drive*[1006]. En el presente trabajo no se discute que los archivos que estén guardados en un formato físico no sean bienes digitales, sino que no se les aplica el artículo 96 de la LOPDGDD. El mundo digital está en constante evolución, lo que hace que no sea fácil identificar cuándo estamos realmente ante un activo digital[1007], y esa puede ser la razón por la que el legislador estatal ha optado por no realizar un listado de dichos contenidos digitales en la LOPDGDD, aunque esta opción del legislador puede crear problemas interpretativos en el futuro.

Podrán acceder a contenidos digitales gestionados por prestadores de servicios de la sociedad de la información de la persona fallecida las personas vinculadas al fallecido por razones familiares o de hecho y sus herederos; el albacea testamentario así como aquella persona o institución a la que el fallecido hubiese designado expresamente para ello; en el caso de los menores sus representantes legales o, en el marco de sus competencias, el Ministerio Fiscal; y, en el caso de que el fallecido fuese una persona con discapacidad, el designado para el ejercicio de funciones de apoyo si tales facultades se entendieran comprendidas en las medidas de apoyo que prestase. En cambio, CÁMARA LAPUENTE se ha manifestado en contra de la amplia legitimación que otorga la normativa por defecto, siendo preferible que la legitimación para ejercer esas facultades provenga del difunto[1008]. Siguiendo esta línea, GINEBRA MOLINS afirma que permitir la intervención concurrente de tantas personas legitimadas *ex lege* identificadas de manera tan imprecisa e indeterminada, bastando un vínculo con el fallecido por razones familiares o de hecho salvo prohibición expresa, y con facultades tan amplias resultar excesivo. Por ello, la autora defiende que resultaría preferible la regla del no acceso salvo que se haya manifestado lo contrario[1009].

[1005] SANTOS MORÓN, M.J., "La denominada "herencia digital": ¿necesidad de regulación? Estudio de Derecho español y comparado", *Cuadernos de Derecho transnacional*, Vol.10, Núm.1, 2018, pp. 416 y 422

[1006] MORALEJO IMBERNÓN, N., "El testamento digital en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *Anuario de derecho civil*, 2020, p. 255, disponible en: https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-2020-10024100281

[1007] TOYGAR, A.; TAPIE, C.E.; ZHU, J., "A new asset type: digital assets", *Journal of International Technology and Information Management*, Vol. 22, Núm. 4, 2013, p. 118

[1008] CÁMARA LAPUENTE, S., "La sucesión mortis causa en el patrimonio digital", *cit.*, pp.421-422

[1009] GINEBRA MOLINS, M.E., "Voluntades digitales: disposiciones mortis causa", en ARROYO AMAYUELAS, E. y CÁMARA LAPUENTE, S., *El derecho privado en el nuevo paradigma digital*, Marcial Pons, Madrid, 2020. pp. 233-234

En el derecho foráneo podemos citar el caso del legislador francés, el artículo 40.1 de la Ley nº 78-17 de 6 enero de 1978 relativa a "la Informática, archivos y libertades" añadido por el artículo 63.2 de la Ley nº 2016-1321 de 7 octubre de 2016 "para una república digital" recoge que los derechos del interesado se extinguen por su muerte. No obstante, la normativa permite que el titular de los datos pueda definir directrices relativas al almacenamiento, supresión y comunicación de sus datos personales para el caso en que fallezca, nombrando un responsable para que lleve a cabo dichas instrucciones. El legislador francés utiliza el término de directrices, no habla de unas voluntades digitales como en el caso de la normativa catalana que se indicará más adelante.

Las directrices pueden ser generales o específicas. Las primeras se refieren a todos los datos personales del titular, mientras que las segundas solo contemplan determinados tipos de datos personales que están registrados ante proveedores de servicios particulares[1010]. Las directrices generales atañen al conjunto de los datos personales del titular y pueden ser registradas ante un tercero digital de confianza certificado por la Comisión Nacional de la Informática y Libertades (CNIL)[1011] en un registro único cuyos términos y condiciones se fijan por decreto en el Consejo de Estado, previo dictamen motivado y publicado de la CNIL.

Las directrices particulares son instrucciones que el interesado otorga directamente a los proveedores de servicios particulares para los datos que tratan estos últimos. Es decir, son instrucciones que se otorgan a concretos prestadores de servicios de internet sobre los datos que son responsables. Estas instrucciones no pueden ser el resultado de la mera aceptación de los términos y condiciones generales que el interesado hubiese aceptado, debe tener libertad para expresar su voluntad.

La persona que otorga las directrices puede designar a una tercera persona para que ejecute las instrucciones. En el caso de que el titular de los datos no hubiese designado a una persona para la ejecución de las directrices, tanto generales como particulares, los herederos podrán ejercer los derechos mencionados en la medida necesaria para la liquidación y partición de la herencia. A su vez, los herederos pueden recibir información sobre activos digitales, hacer que se cierren las cuentas de usuario del difunto, oponerse a la continuación del procesamiento de sus datos personales o hacer que se actualicen. El problema es que la normativa francesa solo se refiere a los datos personales, a diferencia de la LOPDGDD que diferencia los datos personales de los

[1010] ORDELIN FONT, J.L. y ORO BOFF, S., "Bienes digitales personales y sucesión mortis causa: la regulación del testamento digital en el ordenamiento jurídico español", *Revista de derecho (Valdivia)*, Vol. 33, Núm. 1, 2020, p. 121

[1011] La Comisión Nacional de la Informática y Libertades o "*Commission Nationale de l'Informatique et des Libertés*" (CNIL) es la autoridad de protección de datos en Francia.

contenidos digitales del fallecido, lo cual podría dejar ciertos datos no personales fuera de la aplicación de la normativa francesa[1012].

A diferencia del artículo 3 de la LOPDGDD, el artículo 96 de la LOPDGDD introduce el concepto del albacea, lo cual es un claro ejemplo del sentido sucesorio que le ha querido otorgar el legislador estatal al presente artículo. No obstante, puede cuestionarse la adecuación del uso este término, dado que el albacea es nombrado por el testador[1013], y si el testamento digital no es realmente un testamento, no habrá albaceas. A su vez, es cuestionable que la identidad digital que tenía el fallecido en las redes sociales sea transmisible aunque el artículo 96.2 de la LOPDGDD sí que permite expresamente decidir acerca del mantenimiento o eliminación de los perfiles personales en las redes sociales de las personas fallecidas[1014]. Aunque el artículo 96 de la LOPDGDD utilice el término "testamento", el contenido de dicho artículo va más allá de la definición que otorga el Código Civil al concepto tradicional del testamento[1015], siendo más adecuado nombrarlo como la voluntad digital del fallecido tal y como lo hace la Ley 10/2017, de 27 de junio, de las voluntades digitales y de modificación de los libros segundo y cuarto del Código Civil de Cataluña[1016].

Se entiende por *"*voluntades digitales en caso de muerte" las disposiciones establecidas por una persona para que, después de su muerte, el heredero o el albacea universal, en su caso, o la persona designada para ejecutarlas actúe ante los prestadores de servicios digitales con quienes el causante tuviese cuentas activas[1017]. En base a lo dispuesto en el preámbulo de la citada ley, para gestionar la huella en los entornos digitales cuando la persona muere y para evitar daños en otros derechos o intereses tanto de la propia persona como de terceros, las personas pueden manifestar sus voluntades digitales para que el heredero, el legatario, el albacea, el administrador o la persona designada para su ejecución actúen ante los prestadores de servicios digitales después de su muerte[1018].
Mediante estas voluntades digitales, las personas pueden ordenar las acciones que consideren más adecuadas para facilitar que la desaparición física y la pérdida de

[1012] En este sentido: CÁMARA LAPUENTE, S., "La sucesión mortis causa en el patrimonio digital", *cit.*, p.390; SANTOS MORÓN, M.J., "La denominada "herencia digital": ¿necesidad de regulación? Estudio de Derecho español y comparado", *cit.*, p.433

[1013] Artículo 892 del CC

[1014] El Tribunal Federal de Justicia de Alemania (BGH) en su sentencia ZR 183/17 del 12 de julio de 2018 resolvió que los padres de una chica menor fallecida en el metro de Berlín en extrañas circunstancias que hacían pensar que podía tratarse de un suicidio, estaban legitimados para acceder a su cuenta de Facebook para indagar sobre la muerte de la misma al haberse transmitido el contrato que firmo la fallecida con la plataforma a su herederos, en este caso, sus padres. Esto es, se consideró que la posición contractual de la hija era transmisible a los padres.

[1015] Artículo 667 del CC "*el acto por el cual una persona dispone para después de su muerte de todos sus bienes o de parte de ellos se llama testamento*".

[1016] BOE núm. 173, de 21 de julio de 2017.

[1017] Artículo 6 de la Ley 10/2017 que modifica el artículo 411-10 del Código civil de Cataluña

[1018] Uno de los mayores problemas que surge en este punto es que, debido a la falta de una normativa homogeneizada a nivel internacional, los prestadores de servicios digitales pueden tener diferentes políticas sobre lo que le sucede con la identidad digital y activos digitales del interesado al morir. Véase: CONWAY, H. y GRATTAN, S., "The "New" Property: Dealing with Digital Assets on Death", Modern Studies in Property Law, vol. 9, 2017, p. 114

personalidad que supone la muerte se extiendan igualmente a los entornos digitales y que eso contribuya a reducir el dolor de las personas que les sobrevivan y de las personas con las que tengan vínculos familiares, de afecto o amistad, o bien que se perpetúe la memoria con la conservación de los elementos que estas determinen en los entornos digitales o con cualquier otra solución que consideren pertinente en ejercicio de la libertad civil que les corresponde en vida.

La persona a quien se encarga la ejecución de las voluntades digitales no tiene un cometido mínimo o esencial, la ley permite diversas posibilidades: comunicar la muerte a los prestadores de los servicios digitales, solicitarles la cancelación de cuentas, y solicitarles que ejecuten lo previsto contractualmente para el caso de muerte del titular, incluida la posibilidad de obtener una copia de los archivos correspondientes. La ley no obliga a que se borre en todo caso la presencia del difunto en Internet, sino que su cometido podría ser todo lo contrario, debiendo asegurarse que dicha presencia no desaparezca[1019].

La normativa también contempla en su artículo 1, que modifica el artículo 222-2 del Código civil de Cataluña, la posibilidad de otorgar un poder mediante el cual el poderdante podrá establecer la gestión de sus voluntades digitales y su alcance para que, en caso de pérdida sobrevenida de la capacidad, el apoderado actúe ante los prestadores de servicios digitales con quienes el poderdante tenga cuentas activas a fin de gestionarlas y, si procede, solicitar su cancelación. Adecuando este apartado a la Ley 8/2021, una persona podrá otorgar un poder en previsión o apreciación de la concurrencia de circunstancias que puedan dificultarle el ejercicio de su capacidad jurídica en igualdad de condiciones con las demás, para que el apoderado gestione su voluntad en el mundo digital. El problema es que la aplicabilidad de este artículo está limitada a la vida de la persona con discapacidad, no se refiere en ningún momento al caso en que fallezca el usuario, el titular de la cuenta estará vivo cuando el apoderado tenga que ejecutar las voluntades digitales del primero.

El concepto de "voluntades digitales en caso de muerte" que regula la legislación catalana puede tener un contenido sucesorio y/o no sucesorio. La persona tiene la posibilidad ordenar el destino de sus bienes digitales en caso de muerte como puede gestionar el destino del resto de su patrimonio analógico[1020]. Junto a estas disposiciones sucesorias, el causante puede prever otras disposiciones no sucesorias, a modo de instrucciones a determinadas personas para que realicen ciertas actuaciones en relación

[1019] RUDA GONZÁLEZ, A., "Vida más allá de la muerte (digital). La protección de las voluntades digitales en la reforma del derecho catalán", en ANGLÈS JUANPERE, B.; BALCELLS PADULLÉS, J.; BORGE BRAVO, R.; DELGADO GARCÍA, A.M.; FIORI, M.; BARCELÓ, M.J.; MANTELERO, A.; MARSAN RAVENTÓS, C.; PIFARRÉ DE MONER, M.J. y VILASAU SOLANA, M. (coords). *Managing risk in the digital society*, Huygens, Barcelona, 2017, p.231

[1020] En base a GINEBRA MOLINS, los bienes que constituyen el patrimonio digital de la persona y que no se extinguen con su muerte se integran en su herencia, por ello, no es posible hablar de la "herencia digital" como algo distinto de la "herencia analógica". Véase: GINEBRA MOLINS, M.E., "Voluntades digitales en caso de muerte", *Cuadernos de derecho transnacional*, Vol. 12, Núm. 1, 2020, p. 916

con el rastro digital[1021] que deja tras de sí, lo cual cobra especial relevancia para la gestión de las redes sociales[1022].

Ante esta regulación, en el voto particular que formula la Magistrada ROCA TRÍAS a la Sentencia dictada en el recurso de inconstitucionalidad núm. 4751-2017[1023], se pone de manifiesto que el documento de voluntades digitales no es un testamento, el formato digital de determinados contenidos en archivos o el lugar donde se encuentran ubicados no los distingue del resto de bienes que puedan integrar el caudal relicto. Al fallecimiento del otorgante del documento de voluntades digitales, su herencia comprenderá todos sus bienes, derechos y obligaciones que no se hayan extinguido por su fallecimiento y su transmisión se producirá, en cualquier caso, por la voluntad que este haya manifestado en testamento y, a falta del mismo, por disposición de la Ley. El documento de voluntades no contiene una verdadera ordenación de la sucesión, ni tan siquiera de los materiales o archivos digitales del causante, que con independencia del soporte digital en el que se encuentran, en todo caso forman parte del caudal hereditario y son objeto de la sucesión. Lo que recoge realmente el documento es la voluntad del fallecido respecto a la realización de actividades muy concretas que están directamente relacionadas con el ejercicio de derechos personalísimos de carácter no patrimonial no transmisibles mortis causa, como las de comunicar a los prestadores de servicios digitales su defunción; solicitar la cancelación de las cuentas activas o que ejecuten las cláusulas contractuales o que se activen las políticas establecidas para los casos de defunción y, si procede, que libren una copia de los archivos digitales que estén en sus servidores.

En base a todo lo anterior, si el testamento digital se refiere a los contenidos gestionados por prestadores de servicios de la sociedad de la información, el interesado no podrá utilizar esta vía para determinar su voluntad relativa al acceso y, en su caso, su rectificación o supresión de sus datos personales. Esto es, el ejercicio *post mortem* de los citados derechos no se reflejará en el testamento digital. Cabría preguntarse si, en el específico ámbito sanitario, esta voluntad puede ser recogida en el documento de voluntades anticipadas del interesado.

Al igual que ocurre con el testamento digital, el testamento vital no es realmente un testamento, pero permite reflejar la voluntad y deseos de una persona en el ámbito sanitario, de ahí que sea más adecuado el término de voluntades anticipadas. Sería oportuno recoger todas las voluntades sanitarias en un único documento, separando los respectivos tratamientos (tratamientos médicos y tratamientos de los datos relativos a la

[1021] También se ha referido a dichos datos como restos digitales. Véase: MORSE, T. y BIRNHACK, M., "The posthumous privacy paradox: Privacy preferences and behavior regarding digital remains", *New Media & Society*, Vol. 24, Núm. 6, 2022, p.1344

[1022] GINEBRA MOLINS, M.E., "Voluntades digitales: disposiciones mortis causa", *cit.*, pp. 219-220

[1023] ROCA TRÍAS, E., "Voto particular discrepante que formula la Magistrada doña Encarnación Roca Trías a la Sentencia dictada en el recurso de inconstitucionalidad núm. 4751-2017", *tribunalconstitucional*, 17 de enero de 2019, p. 4 disponible en: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_002/2017-4751VPS.pdf

salud), como en el caso del consentimiento informado y el consentimiento del interesado que pueden ir en un único documento siempre que se separen adecuadamente para que el paciente/interesado no sea confundido.

Como critica al planteamiento descrito, podría argumentarse que la aplicación de las voluntades anticipadas está limitada a la vida del sujeto. Sin embargo, la normativa[1024] también contempla que el sujeto exprese su decisión respecto a materias como la donación de órganos para el caso de su defunción. Tomando dicha realidad como ejemplo, se podría defender la creación de unas voluntades anticipadas más amplias que también recojan la voluntad del interesado respecto a sus derechos relativos a la protección de datos personales para el caso en que fallezca.

El artículo 3.2 de la LOPDGDD habla de "instrucciones", "requisitos y condiciones para acreditar la validez y vigencia de estos mandatos e instrucciones" y la posibilidad de introducir un "registro", para la gestión de los datos personales de las personas fallecidas, tomando como base un real decreto que, a día de hoy, no se ha desarrollado. De la lectura del presente artículo se puede deducir que el legislador tenía como objetivo crear un instrumento jurídico que, cuatro años más tarde, sigue sin existir.

Es cierto que el documento de instrucciones previas o voluntades anticipadas está ideado para que una persona anticipadamente refleje su voluntad en cuanto al cuidado, tratamiento y destino de su cuerpo o partes del mismo. Pero el párrafo 6 de la exposición de motivos de la Ley 7/2002 del País Vasco indica que se ha optado por un modelo de voluntades anticipadas cuyo contenido sea el más amplio posible y permita abarcar desde la manifestación de los propios objetivos vitales y valores personales hasta instrucciones sobre los tratamientos que se desean o se rechazan, así como otras previsiones relacionadas con el final de la vida.

Por tanto, actualmente, y mientras no se desarrolle ningún real decreto al objeto de regular esta materia contemplada en la Ley orgánica, el documento de las voluntades anticipadas constituye, en nuestra opinión, un instrumento jurídico adecuado para que el interesado pueda plasmar su voluntad en cuanto al tratamiento de sus datos relativos a la salud tras su fallecimiento, quedando todas sus pretensiones sanitarias juntas en un único documento. En cuanto a las personas mayores con discapacidad, podrán, con el apoyo que precisen, indicar en el documento de voluntades anticipadas cuál es su

[1024] Artículo 11.1 de la LBAP: "*Por el documento de instrucciones previas, una persona mayor de edad, capaz y libre, manifiesta anticipadamente su voluntad, con objeto de que ésta se cumpla en el momento en que llegue a situaciones en cuyas circunstancias no sea capaz de expresarlos personalmente, sobre los cuidados y el tratamiento de su salud* ***o, una vez llegado el fallecimiento, sobre el destino de su cuerpo o de los órganos del mismo***"; Párrafo 6 de la exposición de motivos de la Ley 7/2002 del País Vasco: "*Ante todo hay que decir que se ha optado por un modelo de voluntades anticipadas cuyo contenido sea el más amplio posible y permita abarcar desde la manifestación de los propios objetivos vitales y valores personales hasta instrucciones más o menos detalladas sobre los tratamientos que se desean o se rechazan, pasando por la designación de uno o varios representantes que sean los interlocutores del médico o del equipo sanitario llegado el caso,* ***así como otras previsiones relacionadas con el final de la vida, tales como la donación de órganos o del propio cuerpo****, las autopsias clínicas o similares*".

voluntad en cuanto al tratamiento de sus datos relativos a la salud que pueda realizarse tras su muerte.

CONCLUSIONS

These conclusions are intended to synthesize the answers to the research questions I posed at the beginning of my research about the key elements of health data protection of the elderly.

1. As a result of the analysis we carried out on the European harmonized legal instruments as well as at the national level, we can say that the data subject's consent is not a sufficiently robust control tool in the digital age to guarantee the right to data protection of personal data. Complementary strategies must be established incorporating specific measures to respect the right to data protection throughout the entire life cycle of the personal data, be it a system, a service, a hardware or software product, or even a process. In this sense, we consider that the doctrine has not paid enough attention to the data protection by design and by default (DPbDD) instrument of article 25 GDPR, which in our opinion can prevent harm and may help to establish more respectful data protection policies and cultures, changing the current reality. Vision of prevention and risk reduction should be adopted operating from the design and development of technological tools that respect the right to protection of personal data of future users.

One of the main innovative factors of GDPR consists on the compliance of the data protection by design and by default, which is accredited through a specific certification tool. By incorporating articles 25 and 42 of the GDPR, the legislator has introduced a salient instrument that must be applied in practice, ceasing to promote only the individualist system of the data subject's consent, in which all the weight falls on the data subject and not on the controller. The controller must implement “appropriate technical and organizational measures” and integrate “the necessary guarantees” to apply the principles contained in the GDPR, and thus protect the right to protection of personal data of the data subject from the moment of design of data collection strategies. In the same way, when a computer application, a service or a device goes on the market, the most stringent settings must be applied by default, without the data subject having to take any action.

Data protection compliant measures from design and by default must be an essential aspect to include in any business or research plan. If data subjects are sure that their right to data protection will be respected, they will trust online services and opt for said services or products in the future. Therefore, data protection by design and by default can also be identified as a business strategy that benefits both parts. Certification mechanisms are an appropriate way to demonstrate that the data controller complies the obligation of article 25 of the GDPR, and therefore, it becomes a tool to ensure that data subjects trust the processing of personal data that data controllers will carry out, as it is a mechanism created by the European legislator to demonstrate compliance with the personal data protection regulations and thus generate a feeling of security in data subjects. It is necessary to grant the value that corresponds to the certified mark, so that citizens get used to them and can choose the computer application, service or device that has said certification.

But, even if DPbDD is a marked improvement, by the time data collection and processing must be implemented through the legal basis of data subject's consent, this consent must meet the four analysed requirements (freely given, specific, informed and unambiguous) to be valid.

2. As to the question of whether elderly people with disabilities can give valid consent for the processing of their health data or not, new civil legislation at the national level must be taken into account. With the enforcement of Law 8/2021, of June 2, which reforms civil and procedural legislation to support people with disabilities in the exercise of their legal capacity, elderly with disabilities, are able to grant their consent with the support they need.

Data subjects, with the support they need to make decisions, can express in a notarial deed both at present time and for the future. For that aim, data subjects need to define the regime of action of the person who will provide the support and the security measures they deem appropriate. In the same way, it would be convenient to make a list collecting all the wills, desires and preferences of the data subject in data protection matters. Thus, if in the future they cannot express their will, people in charge (proxies or assistants) will follow what is expressed in that list.

People in charge must support elderly people with a disability so that they can grant their consent after being duly informed, taking into account the accessibility of the information (short and simple sentences, large letters, information by layers...). In the most extreme cases where support with representation functions is necessary because data subjects cannot express their will, people in charge of supporting them must find out their will, wishes and preferences in order to give the consent or not. In the case of elderly people, finding out their values and preferences should not be a difficult task, taking into account their lifelong choices.

So, in order to do the processing, elderly people with disabilities will have to grant their consent with the support they need or, in the most extreme cases, through representation. When this consent does not exist, also applicable to the case in which the data subject's desire cannot be deduced, it must be analysed if another legal basis of article 9.2 GDPR may be applicable, which would make the processing lawful.

3. Innovative digital health solutions can be used without the subject being conscious of the harvesting of data that is taking place through IoT and connected devices. The question is could data processing for health monitoring purposes on an elderly with disabilities be carried out without data subject's consent? Think for example of a smart device measuring some chronic condition of the data subject that could be as standardized as the use of pacemakers in healthcare. In our opinion, processing of health data made through these objects could be based on article 9.2.h) of GDPR, applicable when processing is necessary for the purposes of preventive or occupational medicine, if carried out through connected devices. In any case, this processing would have to respect the principles of GDPR and appropriate technical and organisational measures should be introduced to guarantee the integrity, availability and confidentiality of the

data. In this sense, although the processing could be based on article 9.2.h) of GDPR, it will not be possible to collect and analyse data subject's personal data 24 hours per day, because this processing wouldn't respect the GDPR.

Therefore, it can be affirmed that, the only way in which the concept of best interest of the elderly person with a disability could be applied is when the will of the data subject is unknown, the processing cannot be justified on other legal basis, and the said processing is vital for the person. This would mean that a certain health data processing is essential for the life and well-being of the elderly person with a disability. The processing will not be justified if it is not essential and can be replaced.

4. Referring to health data processing for research purposes, it must be said that, although the GDPR promised to harmonise the regulation for the processing of personal data for research purposes, it did not fully fulfil its objective as article 9.4 of GDPR delegated on Member States the capacity to develop their own regulations in this area.

The Spanish legislator chose to regulate the processing of personal data for health research purposes in the Seventeenth Additional Provision of the Organic Law 3/2018 on Protection of Personal Data and Guarantee of Digital Rights (known as LOPDGDD).

Within this Additional Provision, as much as four legal bases are identified to treat health data for research purposes: (I) data subject's consent, (II) situations of exceptional relevance and seriousness for public health, (III) reuse of personal data for purposes or research areas related to the area in which the initial study is scientifically integrated, (IV) use of pseudonymised personal data. Data subject's consent can be formulated in a broad manner, allowing, for example, data collected for lung cancer research purposes to be extended to the oncology research field. But is debatable if this broad consent complies with the GDPR. Spanish regulation has also been criticized because of lacking proper legislative technique. In the first place it is dubious that research with health data issues should be regulated in an additional provision of an organic law. It is also open to criticism that these security measures that are regulated in letters e), f) and g) of the second section of the 17th.2 A.P of the LOPDGDD, are very difficult to construe due to their complex wording.

Italy regulates this area in two specific articles of the Legislative Decree No. 196 of June 30 2003, the "*Codice*" or Code, separating the processing of health data for medical, biomedical and epidemiological research from the subsequent processing of personal data for statistical or scientific research purposes. Although the article 110 of the Code identifies data subject's consent as the rule for the processing of health data for medical, biomedical and epidemiological research, it introduces two major exceptions: (I) when research is carried out on the basis of legal or regulatory provisions or the Law of the European Union in accordance with article 9.2.j) of the GDPR or when the research is part of a biomedical or health research program contemplated in article 12-bis of Legislative Decree 502/1992; (II) when it is impossible or involves a

disproportionate effort to inform the data subject or it may be impossible or seriously jeopardize the achievement of the research purposes.

Based on article 110-bis of the Code, the Italian Data Protection Authority ("*Garante*") can authorize further processing of personal data for scientific research purposes to third parties who mainly carry out these activities when, for particular reasons, it is impossible to inform the data subject or is likely to make it impossible or seriously affect the achievement of the objectives of the research, provided that appropriate measures are taken to protect the rights, freedoms and interests of the data subject. For all these reasons, although the Italian legislator identifies the consent as the rule for the processing of health data, there are many situations in which it is not necessary to obtain said consent. These exceptions require interpretation, which can create problems for researchers when they carry out their work.

Ireland regulates this matter specifically in its S.I. No. 314/2018 - Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018, which makes Irish system differs positively from the previous two. In the aforementioned law, explicit consent is identified as the legitimising basis for the processing of personal data for health research purposes, being the declaration of consent the only lawful mechanism that allows, in exceptional circumstances, the processing of personal data for research purposes without the explicit consent of the data subject. Although the regulations try to show that the explicit consent is the only legitimising basis of the Irish legal system, nevertheless public interest can also be a legitimizing basis. So that, by introducing the authorization of the HRCDCC as an exception to the explicit consent norm, we can identify two different legitimising bases.

Regarding the processing of personal data for health research purposes that has been carried out in the context of the pandemic, the Spanish data protection agency has not produced any guide that allows knowing how the 17th.2 A.P of the LOPDGDD should be interpreted and applied in a circumstance as exceptional as that caused by COVID-19. Italy has introduced a partial derogation from article 110 of the Code, allowing to process data without the need to present previously the research project and carry out the impact assessment and prior consultation with the Guarantor. In contrast, in Ireland, during the pandemic, the legitimising basis has continued to be the data subject's explicit consent, being the HRCDC's consent declaration the only exception to the rule. The fact that all these application assessment meetings are available on the official HRCDC website is a great example of transparency that must be underlined.

Despite the fact that none of the three systems is perfect, in our opinion, the Irish model stands out positively from the other two for being the most appropriate one. Ireland has opted to create a specific law for such an important area, and its wording correct, which does not require carrying out the arduous task of interpretation that the two remaining models do. In addition, the control that the HRCDC have done during the pandemic and its advertising is truly exemplary, becoming a great control tool citizen's fundamental right to data protection. Taking Ireland as an example, it could be argued that the GDPR

must be reformed to harmonise health research, the legal bases must be clear and equal for all European countries. Likewise, it is necessary to explicit which are the appropriate and specific measures in place to protect the interests and fundamental rights of data subjects, especially elderly subjects with disabilities.

5. Data subjects are granted new rights at the new data protection Regulation. Actually, data subjects have the right of access, right to rectification, right to erasure, right to be forgotten, right to restriction of processing, right to data portability and to object regulated between articles 15 and 21 of the GDPR. Likewise, article 22 of the GDPR introduces the right not to be subject to a decision based solely on automated processing, which more than a right could be understood as a prohibition for data controllers.

The right of access refers to the right of the data subjects to obtain from the controllers confirmation as to whether or not personal data concerning them is being processed and access to the personal data and some information. By this right, patients can access to their health data, which is located in their medical records.

Patients who verify that the information contained in their clinical history is not correct or is incomplete, will have the right to request rectification. Once the rectification request has been made, it will be up to the health professional to determine whether the data have to be rectified or not. Health professionals must analyse the circumstances of each case, always taking into account medical criteria, to assess if this change may condition or harm the patient's health care.

The right to erasure means that patients will have the right to request the deletion of their health data. The exercise of this right has its limitations; the data which is contained in medical records must be kept for a minimum period of five years, although this period can change depending on the autonomic regulation, the deletion of the data cannot be done when the health of the patient could be harmed as a result in the future, and other legitimate interests of third parties.

Unlike the previous right to erasure, the right to be forgotten refers to the possibility of limiting the universal and indiscriminate dissemination of personal data in general search engines when the information is obsolete or no longer of relevance or public interest, even if the original publication is legitimate, as first stated by the European Court of Justice in the Google Spain vs. Mario Costeja case. Due to its nature, in the health field, in the vast majority of cases, the right to erasure will apply instead the right to be forgotten when the patients want to proceed with the deletion of their personal data, since patient's health data are not commonly available to citizens on the Internet.

The patient may exercise the right to restriction of processing of his or her health data while the controller decides on the appropriateness of the request. Right to retention could also apply when the patient wants his or her data to be retained even if the processing may be unlawful or unnecessary; when the controller no longer needs the

data, but the patient needs it to make or defend claims; and while the controller decides if the right to object is applicable.

The new right to data portability is especially important for granting freedom of choice, since it allows patients to transfer their health data to another health centre within their country or abroad. Portability of health records at public and private services could be a great improvement for patients, even if it is not applicable as a right as long as the data processing in this context is not usually based on the consent of the subject.

Through the right to object, patients expose their eventual refusal to have their health data processed. After having exercised this right, controllers must stop carrying out the processing unless they are able to produce compelling legitimate reasons that prevail.

Finally, the GDPR includes in the article 22 the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects on data subjects or significantly affects them in a similar way. Decisions may only be made based solely on the automated processing of data when article 9.2.a) or article 9.2.g) of the GDPR is applicable and the appropriate measures have been taken to safeguard the rights and freedoms and legitimate interests of data subjects. That is, this processing will only be allowed when data subjects have given their explicit consent or the processing is necessary for reasons of essential public interest.

The rights that have been recognized by the GDPR are fundamental personal rights, which mean that they must be exercised personally by the data subject. However, after the entry into force of Law 8/2021, an interpretation of article 12.1 of the LOPDGDD must be done in accordance with the reform. So that, elderly people with disabilities will be the ones who are called to exercise these rights in the first place with the support they need. Only in the most extreme cases, where they cannot express their will, the consent will be given by representation. But even in these cases, assistants in charge of supporting elderly people with disabilities must find out their will, wishes and preferences, based on their livelong values and choices. The right way to guarantee respect of their genuine wishes is to indicate in a notarial deed that support to be granted in the field of data protection should be provided, following the instructions and the actions the person who will provide the support can take and introducing a list that reflects the will, wishes and preferences of the data subject. The person in charge of granting the support should respect always that will.

When a right is exercised with the support of an assistant, the name, surname and identification number of this person must be indicated together with the data of the data subject, attaching, where appropriate, a copy of the power of attorney or the resolution of the judicial support measure. However, both the Spanish Data Protection Agency and The Basque Data Protection Agency keep the section of “legal representative” on their current forms on their respective official pages. This reference should be removed after the reform operated by Law 8/2021 and substituted by some reference of this sort: “data

of the person who grants support for the exercise of data subject's rights", in order to collect the case of elderly people with disabilities.

Although the GDPR establishes that the data protection regulation does not apply to the processing of personal data of deceased people, it legitimises Member States to establish regulations for this type of processing. Therefore, the European legislator has renounced to harmonise the regulation on the processing deceased's data.

Article 3 of the LOPDGDD states that proxies linked to the deceased person for family or de facto reasons, as well as their heirs, may contact the controller in order to request the access to personal data of the defunct, and when appropriate, they can claim for the rectification or erasure of their health data, provided that the deceased person had not expressly prohibited it or so established by law. In the health field, according to the interpretations of the Spanish Data Protection Agency and the Basque Data Protection Agency, they will be entitled to access the clinical history of the deceased, unless there is an express opposition of the former data subject. Those who do not prove a relationship such as spouse, common law partner, relative or some other factual link, will be considered as third parties, and like the relatives affected by the express opposition of the deceased, they will only access the clinical history when there is a risk for their own health, and they will only access clinical data of the deceased strictly necessary to protect that legal right. As a criticism, it could be argued that the legitimation granted by the Law 41/2002 and Basque Decree 38/2012 to the relatives of the deceased is excessive, because it legitimises a large crowd of people without legal or medical justification.

Regarding the possibility of data subjects to reflect their will for the *post mortem* exercise of their rights, and thus deal with the aforementioned legitimation, it would be legally relevant if this choice could be reflected in the advance directives regulated in the Law 41/2002, and the Basque Law 7/2002. Though the application of advance directives is regularly limited to the life of a person, the regulations also allow the possibility to express other decisions to be fulfilled after death, such as organ donation.

In our opinion, as long as there is a legal vacuum on this matter, the document of advance directives could be an adequate legal instrument for data subjects to express their will for the processing of their health data made after their death. So that, people could order their health directives together in a single legal binding document. As for the elderly people with disabilities, they may also indicate in the advance directives, with the support they need, their will regarding to the post-mortem processing of their health data.

BIBLIOGRAFIA

- **LIBROS:**

- ALKORTA IDIAKEZ, I., El espacio europeo de datos sanitarios: nuevos enfoques de la protección e intercambio de datos sanitarios, Aranzadi, Pamplona, 2022

- ÁLVAREZ CARO, M., *Derecho al olvido en Internet: El nuevo paradigma de la privacidad en la era digital*, Reus, Madrid, 2015

- ÁLVAREZ HERNANDO, J., *Practicum protección de datos*, Aranzadi, Pamplona, 2018

- APARICIO SALOM, J. y VIDAL LASO, M., *Estudio sobre la protección de datos*, Aranzadi, Pamplona, 2019

- ARLETTAZ, F. y PALACIOS SANABRIA, M.T., *Reflexiones en torno a Derechos Humanos y grupos vulnerables*, Universidad del Rosario, Bogotá, 2015

- BARIFFI, F.J., *El régimen jurídico internacional de la capacidad jurídica de las personas con discapacidad*, Ediciones Cinca, Madrid, 2016

- BARRIO ANDRÉS, M., *Internet de las cosas*, Reus, Madrid, 2018

- BENÍTEZ, R.; ESCUDERO, G.; KANAAN, S. y MASIP, D., *Inteligencia artificial avanzada*, UOC, Barcelona, 2014

- *BERROCAL* LANZAROT, A. I., *Estudio jurídico-crítico sobre la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales: análisis conjunto del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de* abril de 2016 y de la Ley Orgánica 3/2018 de 5 de diciembre, Reus, Madrid, 2019

- BERROCAL LANZAROT, A.I., *Derecho de supresión de datos o derecho al olvido*, Reus, Madrid, 2017

- BESCANSA MIRANDA, R., *Protección jurídica de la persona: estudio práctico de los negocios jurídicos inter vivos y mortis causa tras la reforma de la ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica*, Aferre, Barcelona, 2021

- BHATTACHARYYA, S.B., *A DIY Guide to Telemedicine for Clinicians,* Springer, Singapur, 2017

- BOLOGNINI, L. Y PELINO, E., *Codice della disciplina privacy,* Giuffrè Francis Lefebrve, Milan, 2019

- BOLOGNINI, L. y PELINO, E., *Codice privacy: Tutte le novità del D.LGS. 101/2018,* Giuffrè Francis Lefebrve, Milan, 2018

- BONILLA SÁNCHEZ, J.J., *Personas y derechos de la personalidad*, Reus, Madrid, 2010

- BOTTARI, C., *La salute del futuro: prospettive e nuove sfide del diritto sanitario*, Bolonia University Press, Bolonia, 2020

- BUTLER, R., *The Encyclopedia of Aging*, Springer, Nueva York, 1987

- CAMPOS ACUÑA, C., *Aplicación práctica y adaptación de la protección de datos en el ámbito local: novedades tras el reglamento europeo; el consultor de los ayuntamientos*; Wolters Kluwer, Madrid, 2018

- CANTERO RIVAS, R.; MARTÍNEZ AGUADO, L.C. y MORENO VERNIS, M., *La historia clínica*, Comares, Granada, 2002

- CASSANO, G; COLAROCCO, V; GALLUS, G.B. y M, F.P., *Il proceso di adeguamento al GDPR. Aggiornato al D.lgs. 10 agosto 2018 n.101,* Giufrè Francis Lefebvre, Milan, 2018

- CdE., *Manual de legislación europea de protección de datos,* Oficina de Publicaciones de la Unión Europea, Luxemburgo, 2018

- CICCIA, A., Guida *al Codice Privacy. Come cambia dopo il GDPR e il D. lgs. N. 101/2018,* Wolter Kluwer, Milan, 2018

- CUENCA GÓMEZ, P., *La capacidad jurídica de las personas con discapacidad: el art. 12 de la Convención de la ONU y su impacto en el ordenamiento jurídico español*, Dykinson, Madrid, 2011

- DE LORENZO MONTERO, R., *Derechos y obligaciones de los pacientes: Análisis de la ley 41/2002, de 14 de noviembre básica reguladora de autonomía de los pacientes y de los derechos de información y documentación clínica*, Colex, Madrid, 2003

- DÍAZ ALABART, S., *La protección de los datos y contenidos digitales de las personas fallecidas,* Reus, 2021

- DURÁN CORSANEGRO, E., *La autorregulación de la tutela*, Ramón Areces, Madrid, 2007

- FERNÁNDEZ DE BUJÁN, A., *La reforma de la jurisdicción voluntaria*, Dykinson, Madrid, 2016

- FERNÁNDEZ GONZÁLEZ, M.B., *Sistema de apoyos para personas con discapacidad*. *Medidas jurídico-civiles y sociales*, Dykinson, Madrid, 2021

- FERNÁNDEZ TRESGUERRES, A., *El ejercicio de la capacidad jurídica: comentario práctico de la ley 8/2021, de 2 de junio*, Aranzadi, Pamplona, 2021

- FERRER ROCA, O., *Telemedicina*, Panamericana, Madrid, 2001

- GADDI, A.; CAPELLO, F. y MANCA, M., *EHealth, Care and Quality of Life*, Springer, Berlin, 2014

- GARCÍA SERRANO, A., *Inteligencia artificial. Fundamentos, práctica y aplicaciones*, RC libros, Madrid, 2012

- GARRIGA DOMÍNGUEZ, A., *Nuevos retos para la protección de datos personales. En la era del Big Data y de la computación ubicua*, Dykinson, Madrid, 2016

- GIL GONZÁLEZ, E., *Big data, privacidad y protección de datos*, Imprenta Nacional de la Agencia Estatal Boletín Oficial del Estado, Madrid, 2016

- GOITIA FUERTES, M., *Aplicaciones informáticas de administración de recursos humanos*, Ediciones Paraninfo, Madrid, 2015

- GOMÁ LANZÓN, J., *Ejemplaridad pública*, Taurus, Barcelona, 2015

- GONZÁLEZ GRANDA, P., *Régimen jurídico de protección de la discapacidad por enfermedad mental*, Reus, Madrid, 2009

- GONZÁLEZ OTERO, B. *Interoperabilidad, internet de las cosas y derecho de autor*, Reus, Madrid, 2019

- GONZÁLEZ RAMÍREZ, A. y MORA LIMA, V., *Teleasistencia*, McGraw-Hill, Madrid, 2013

- GUILARTE MARTÍN-CALERO, C., *Comentarios a la Ley 8/2021 por la que se reforma la legislación civil y procesal en materia de discapacidad,* Aranzadi, Pamplona, 2021

- GUILARTE MARTÍN-CALERO, C., *El derecho a la vida familiar de las personas con discapacidad: El Derecho español a la luz del artículo 23 de la Convención de Nueva York*, Reus, Madrid, 2021

- GUTIERREZ MARTÍN, A., *Alfetización digital algo más que ratones y teclas*, Gedisa, Barcelona, 2003

- HANSEN, J.; WILSON, P.; VERHOEVEN, E.; KRONEMAN, M.; KIRWAN, M.; VERHEIJ, R. y VAN VEEN, E. B., *Assessment of the EU Member States' rules on health data in the light of GDPR*, Oficina de publicación de la UE, Luxemburgo, 2021

- HANSEN, M., *Data protection by design and by default à la European General Data Protection Regulation*, Springer, Cham, 2016

- IASESSI, M., *La tutela dei dati personali in ámbito sanitario*, Giuffrè Francis Lefebrve, Milan, 2020

- ISTEPANIAN, R.; LAXMINARAYAN, S.; PATTICHIS, C., *M-health: Emerging mobile health systems*, Springer, Nueva York, 2007

- JOHNSON, J. y SLATER, R., *Ageing and later life*, Sage, Londres, 1993

- LASARTE ÁLVAREZ, C., *Protección jurídica del menor*, Tirant lo Blanc, Valencia, 2016

- LLÁCER, M.R.; CASADO, M. y BUISÁN, L., *Documento sobre bioética y big data de salud: explotación comercialización de los datos de los usuarios de la sanidad pública*, Publicación de la Universidad de Barcelona, Barcelona, 2015

- LÓPEZ CORONADO, M. y DE LA TORRE, I., *Mejora de la calidad asistencial mediante la telemedicina y la teleasistencia*, Díaz de Santos, Madrid, 2014

- LUENGO, J.; GARCÍA-GIL, D.; RAMÍREZ-GALLEGO, S.; GARCÍA, S. y HERRERA, F., *Big Data Preprocessing: Enabling Smart Data*, Springer, Suiza, 2020

- MARTORANA, M., *GDPR e Decreto Legislativo 101/2018. Vademecum del profesionista: obblighi, adempimenti, strumenti di tutela*, Wolters Kluwer, Milan, 2019

- MIERES MIERES, L.J., *El derecho al olvido digital*, Fundación Alternativas, Madrid, 2014

- NÚÑEZ ZORRILLA, M.C., *La asistencia: la medida de protección de la persona con discapacidad psíquica alternativa al procedimiento judicial de incapacitación*, Dykinson, Madrid, 2014

- PELAYO GONZÁLEZ-TORRE, A., *El derecho a la autonomía del paciente en la relación médica*, Comares, Granada, 2009

- PEREÑA VICENTE, M., *La protección jurídica de adultos: el estándar de intervención y el estándar de actuación: entre el interés y la voluntad*, Dykinson, 2018

- PÉREZ RODRÍGUEZ, M.D., *Ley de Protección de datos*, ICB, Madrid, 2017

- PETRINI, C., *Utilizzo di dati nella ricerca biomédica e negli interventi di sanità pubblica in tempo di Covid-19: alcune implicazioni di ética*, Invalsi, Roma, 2021

- REBOLLO DELGADO, L. y SERRANO PÉREZ, M.M., *Introducción a la protección de datos*, Dykinson, Madrid, 2008

- RODRÍGUEZ AYUSO, J.F., *Garantía administrativa de los derechos del interesado en materia de protección de datos personales*, J.M. Bosch Editor, Barcelona, 2021

- ROMERO COLOMA, A.M., *Capacidad, incapacidad e incapacitación*, Reus, Madrid, 2013

- ROUHIAINEN, L., *Inteligencia artificial. 101 cosas que debes saber hoy sobre nuestro futuro*, Planeta, Madrid, 2018

- RUSSELL, S.J. y NORVIG, P., *Inteligencia Artificial: Un Enfoque Moderno*, Pearson Prentice Hall, Madrid, 2004

- SACRISTÁN, J.A., *Medicina centrada en el paciente*, Unión Editorial: Fundación Lilly, Madrid, 2018

- SALAZAR VARELLA, C.E., *El proceso de incapacitación*, Tirant lo Blanch, Valencia, 2021

- SÁNCHEZ GONZÁLEZ, M.P., *Honor, intimidad y propia imagen*, Jurúa, Lisboa, 2017

- SÁNCHEZ-CARO, J. y ABELLÁN, F., *Derechos y deberes de los pacientes: Ley 41/2002, de 14 de noviembre: consentimiento informado, historia clínica, intimidad e instrucciones previas*, Comares, Granada, 2003

- SERRANO GARCÍA, I., *Autotutela: El artículo 223-II del Código Civil y la Convención de Nueva York sobre los derechos de las personas con discapacidad de 2006*, Tirant lo Blanch, Valencia, 2012

- SIMÓN CASTELLANO, P., *El reconocimiento del derecho al olvido digital en España y en la UE: efectos tras la sentencia del TJUE de mayo de 2014*, Bosch, Barcelona, 2015

- TORRES I VIÑALS, J., *Del cloud computing al big data*, Eureca media, Barcelona, 2012

- TRONCOSO REIGADA, A., *La protección de datos personales: en busca del equilibrio*, Tirant lo Blanch, Valencia, 2010

- VILLARINO MARZO, J., *La privacidad en el entorno del cloud computing*, Reus, Madrid, 2018

- VIVAS-TESÓN, I., *Vivir con discapacidad en el contexto de una pandemia: el derecho a tener derechos*, Tecnos, Madrid, 2021

- ZURITA MARTÍN, I., *Protección civil de la ancianidad*, Dykinson, Madrid, 2004

- **CAPÍTULOS DE LIBROS:**

- ALKORTA IDIAKEZ, I., "La protección del derecho a la autodeterminación informativa de los mayores en entornos conectados" en ALKORTA IDIAKEZ, I. y ATIENZA MACÍAS, E., *Soluciones tecnológicas para los problemas ligados al envejecimiento. Reglamento General de Protección de Datos. Hacia un nuevo modelo de Privacidad*, Dykinson, Madrid, 2020, pp.50-51

- ALKORTA IDIAKEZ, I., "Los riesgos del teletrabajo para la protección de los datos personales de los empleados y de los terceros", en RODRÍGUEZ AYUSO, J.F. y ATIENZA MACÍAS, E. (dir), *El nuevo marco legal del teletrabajo en España: Presente y futuro, una aproximación multidisciplinar*, Wolters Kluwer, Madrid, 2021, pp. 24-25

- ÁLVAREZ LATA, N., "Del defensor judicial de la persona con discapacidad", en BERCOVITZ RODRÍGUEZ-CANO, R.(Coord.)., *Comentarios al Código Civil*, Aranzadi, Pamplona, 2021, pp. 535-536

- BELLO JANEIRO, D., "Una mirada crítica sobre la regulación de la autotutela" en PÉREZ VARGAS MUÑOZ, J., *Congreso Internacional de Derecho Civil. La encrucijada de la incapacitación y la discapacidad*, La Ley, Madrid, 2011, pp. 372-373

- CAVOUKIAN, A. y CHIBBA, M., "Privacy Seals in the USA, Europe, Japan, Canada, India and Australia", en RODRIGES, R. y PAPAKONSTANTINOU, V., *Privacy and Data Protection Seals*, Asser, Berlin, 2018, p. 70

- DE AMUNÁTEGUI RODRÍGUEZ, C., "El protagonismo de la persona con discapacidad en el diseño y gestión del sistema de apoyo", en: SALAS MURILLO, S. y MAYOR DEL HOYO, M.V. (dir)., *Claves para la adaptación del ordenamiento jurídico privado a la Convención de Naciones Unidas en materia de discapacidad*, Tirant lo Blanch, Valencia, 2019, pp. 125 y 150

- DE SALAS MURILLO, S., "De la autocuratela", en GUILARTE MARTÍN-CALERO, C. (dir)., *Comentarios a la ley 8/2021 por la que se reforma la legislación civil y procesal en materia de* discapacidad, Aranzadi, Pamplona, 2021, p. 703

- DUASO CALÉS, R., "Los principios de protección de datos desde el diseño y protección de datos por defecto", en PIÑAR MAÑAS, J.L., *Reglamento General de Protección de Datos. Hacia un nuevo modelo de Privacidad*, Reus, Madrid, 2016, pp. 3010-316

- FERNÁNDEZ SÁNCHEZ, C. y RECIO GAYO, M., "Certificación en protección de datos personales", en PIÑAR MAÑAS, J.L., *Reglamento General de Protección de Datos. Hacia un nuevo modelo de Privacidad*, Reus, Madrid, 2016, pp.413-423

- GACÍA RIPOLL MONTIJANO. M., "El consentimiento al tratamiento de datos personales", en GONZÁLEZ PACANOWSKA, I. y CASTILLA BAREA, M., *Protección de datos personales*, Tirant lo Blanch, Valencia, 2020, p. 155

- GARCÍA MEXÍA, P. y PERETE RAMÍREZ, C., "Internet y el Reglamento General de Protección de Datos", en LÓPEZ CALVO, J. (coord), *El nuevo marco regulatorio derivado del Reglamento Europeo de Protección de Datos*, Bosch, Madrid, 2018, p. 180

- GARCÍA RUBIO, M.P., "La reforma de la discapacidad en el Código Civil. Su incidencia en las personas de edad Avanzada", en GREGORACI FERNANÁNDEZ, B. y VELASCO CABALLERO, F. (Ed.), *El derecho de las sociedades envejecidas*, Editorial BOE, Madrid, 2021, pp. 86-92

- GINEBRA MOLINS, M.E., "Voluntades digitales: disposiciones mortis causa", en ARROYO AMAYUELAS, E. y CÁMARA LAPUENTE, S., *El derecho privado en el nuevo paradigma digital*, Marcial Pons, Madrid, 2020. pp. 219-234

- GÓMEZ-JUÁREZ SIDERA, I. y DE MIGUEL MOLINA, M., "La protección de datos de las personas mayores, necesidad y reto para una innovación tecnológica de calidad", en VALERO TORRIJOS, J., *La protección de los datos personales en Internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013, pp.571-586

- GONZÁLEZ PACANOWSKA, I., "El derecho a la portabilidad de los datos personales: control y uso compartido de los datos personales" en GONZÁLEZ PACANOWSKA, I. (coord.), *Protección de datos personales*, Tirant lo Blanch, Valencia, 2020, p. 572

- GUARDA. P., "Art. 110", en D'ORAZIO, R; FINOCCHIARO, G; POLLICINO, O. y RESTA, G., *Codice della privacy e data protection*, Giuffrè Francis Lefebvre, Milan, 2021, p. 1373-1381

- GUILARTE MARTÍN-CALERO, C., "La reinterpretación jurisprudencial de los sistemas de protección a la luz de la convención de Nueva York: El nuevo paradigma de la sala primera", en GUILARTE MARTÍN-CALERO, C. y GARCÍA MEDINA, J., *Estudios y comentarios jurisprudenciales sobre discapacidad*, Aranzadi, 2016, p. 93

- HALLER, S.; KARNOUSKOS, S.; SCHROTH, C., "The internet of things in an enterprise context", en DOMINGUE, J.; FENSEL, D. y TRAVERSO, P. (Eds.), *Future internet symposium*, Springer, Berlin, 2008, p. 14

- HERNÁNDEZ CORCHETE, J.A. "Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos", en PIÑAR MAÑAS, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo de Privacidad*, Reus, Madrid, 2016, pp. 206-207

- LEGERÉN-MOLINA, A., "La relevancia de la voluntad de la persona con discapacidad en la gestión de los apoyos", en: SALAS DE MURILLO, S. y MAYOR DEL HOYO, M. V. (Dir)., *Claves para la adaptación del ordenamiento jurídico privado a la convención de naciones unidas en materia de discapacidad*, Tirant lo Blanch, Valencia, 2019, p. 180

- LLOPIS BENLLOCH, J.C., "Con la muerte digital no se juega: el testamento online no existe", en OLIVA LEÓN, R. y VALERO BARCELÓ, S., *Testamento ¿Digital?*, Colección Desafíos legales, Juristas con futuro, 2016, p. 49

- LÓPEZ AZCONA, A., "Medidas voluntarias de apoyo", en CERDEIRA BRAVO DE MANSILLA, G.; GARCÍA MAYO, M.; GIL MEMBRADO, C. y PRETEL SERRANO, J.J., *Un nuevo orden jurídico para las personas con discapacidad*, Wolters Kluwer, Madrid, 2021, p. 372

- MARTÍNEZ MARTÍNEZ, R. Y ÁLVAREZ RIGAUDIAS, C., "El uso de datos con fines de investigación biomédica (arts.9 y 89 RGPD. Art 9, Disposición Adicional decimoséptima, Disposición final novena y Disposición transitoria sexta LOPDGDD)", en LÓPEZ CALVO, J., *La adaptación al nuevo marco de protección de datos tras el RGPD y la LOPDGDD*, Wolters Kluwer, Madrid, 2019, p. 279

- MINGORANCE GOSÁLVEZ, C., "Delimitación del término "Persona Mayor" en la ley andaluza de atención y protección a las personas mayores", en PÉREZ VARGAS MUNOZ, J. y PEREÑA VICENTE, M., *La encrucijada de la incapacitación y la discapacidad*, Wolters Kluwer, Madrid, 2011, p. 482

- MONJE BALMACEDA, O., "El estado de la cuestión: La guarda de hecho. Instrumento clave en las instituciones de apoyo", en LLEDÓ YAGÜE, F.; MONJE BALMACEDA, O. y GUTIERREZ BARRENENGOA, A., *Estudio básico sobre la guarda de hecho: algunas reflexiones sustantivas y procesales notables de lege data y de lege ferenda*, Dykinson, Madrid, 2019, p. 59

- NICOLÁS JIMÉNEZ, P., y TERRIBAS I SALA, N., "Investigación con datos de carácter personal", en ROMEO CASABONA, C.M (Dir.); NICOLÁS JIMÉNEZ, P., y ROMEO MALANDA, S. (Coord.), *Manual de bioderecho (Adaptado para la docencia en ciencias de la salud y ciencias sociales y jurídicas)*, Dykinson, Madrid, 2022, p. 685, 698 y 700

- ODDONE, M.J. y POCHINTESTA, P., "La cuarta edad: la fragilidad en cuestión", en PAREDES, M. y MONTEIRO, L. (coord)., *Desde la niñez a la vejez: nuevos desafios*, Teseo, Buenos Aires, 2019, p. 325

- OLIVER LALANA, A.; MUÑOZ SORO, J.F., "El mito del consentimiento y el fracaso del modelo individualista de protección de datos", en VALERO TORRIJOS, J. (Coord.), *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica*, Aranzadi, Pamplona, 2013. p. 188

- PALACIOS GONZÁLEZ, D., "Guarda de hecho, curatela o defesor judicial: Buscando el mejor apoyo para las personas con discapacidad psíquica", en CERDEIRA BRAVO DE MANSILLA, G.; GARCÍA MAYO, M.; GIL MEMBRADO, C. y PRETEL SERRANO, J.J., *Un nuevo orden jurídico para las personas con discapacidad*, Wolters Kluwer, Madrid, 2021, p. 429

- PARRA LUCÁN, M.A., "La guarda de hecho de las personas con discapacidad", en DE SALAS MURILLO, S. (Coord.)., *Los mecanismos de guarda legal de las personas con discapacidad tras la convención de naciones unidas*, Dykinson, Madrid, 2013, p. 255

- PEREÑA VICENTE, M., "Una contribución a la interpretación del régimen jurídico de las medidas de apoyo ene l ejercicio de la capacidad jurídica consagradas en la Ley 8/2021 de 2 de junio", en PEREÑA VICENTE, M., *El ejercicio de la capacidad jurídica por las personas con discapacidad tras la Ley 8/2021 de 2 de junio*, Tirant lo blanch, Valencia, 2022, p.172

- PENASA, S. y TOMASI, M., "The Italian way for research biobanks after GDPR: hybrid normative solutions to balance the protection of individuals and freedom of research", en SLOKENBERGA, S., TZORTZATOU, O., y REICHEL, J., *GDPR and biobaking: individual rights, public interest and research regulation across Europe,* Springer, Suiza, 2021, p. 318

- RECOVER BALBOA, T., "Hacia la reforma del Código Civil y la Ley de Enjuiciamiento Civil en materia de discapacidad", en: GARCÍA GARNICA, María del Carmen y ROJO ÁLVAREZ-MANZANEDA, R., *Nuevas perspectivas del tratamiento jurídico de la discapacidad y la dependencia*, Dykinson, Madrid, 2014, p. 20

- RODRÍGUEZ AYUSO, J.F., "Derechos del interesado como persona física propietaria de los datos personales", en GARCÍA ÁLVAREZ, L., *El mercado único en la unión europea*, Dykinson, 2019, p. 220

- RUDA GONZÁLEZ, A., "Vida más allá de la muerte (digital). La protección de las voluntades digitales en la reforma del derecho catalán", en ANGLÈS JUANPERE, B.; BALCELLS PADULLÉS, J.; BORGE BRAVO, R.; DELGADO GARCÍA, A.M.; FIORI, M.; BARCELÓ, M.J.; MANTELERO, A.; MARSAN RAVENTÓS, C.; PIFARRÉ DE MONER, M.J. y VILASAU SOLANA, M. (coords). *Managing risk in the digital society*, Huygens, Barcelona, 2017, p.231

- VALCÁRCEL TEIJEIRO, N. "Protección de datos de salud e investigación hospitalaria", en GÓMEZ PIQUERAS, C.; MARTÍNEZ MARTÍNEZ, R.; PÉREZ GÓMEZ, J.M.; ROMEO CASABONA, C.M.; SÁNCEZ CARP, J. y VALCÁRCEL TEIJEIRO, N. *Protección de datos e investigación médica*, Aranzadi, Pamplona, 2009, p. 103

- **ARTÍCULOS:**

- ABAD ALCALÁ, L., "Diseño de programas de e-inclusión para alfabetización mediática de personas mayores Comunicar", *Revista científica iberoamericana de comunicación y educación*, Núm. 42, 2014

- ALKORTA IDIAKEZ, I., "Regulación del tratamiento de los datos en proyectos de investigación sanitaria, en especial, en la aplicación de las tecnologías Bigdata", *Revista de derecho y genoma humano*, Núm. Extra 1, 2019

- ÁLVAREZ ROYO-VILLANOVA, S., "Voluntad y consentimiento informado en la Ley para el apoyo a las personas con discapacidad", *El notario del siglo XXI: revista del Colegio Notarial de Madrid*, Núm. 100, 2021

- AREA MOREIRA, M., "La alfabetización digital y la formación de la ciudadanía del siglo XXI", *Revista Integra Educativa*, Vol. 7, Núm. 3, 2014

- ARENAS RAMIRO, M., "Pasaporte Covid, ¿libertad de circulación de forma segura o discriminación y privacidad en juego?", *La Ley privacidad*, Núm.8, 2021

- ARNAU MOYA, F., "Aspectos polémicos de La ley 8/2021 de medidas de apoyo a las personas con discapacidad", *Revista Boliviana de Derecho*, Núm. 33, 2022

- ARROYO AMAYUELAS, E., "El deterioro cognitivo en la vejez. Entre la vulnerabilidad y la discapacidad", *Revista de Bioética y Derecho*, Núm. 45, 2019

- AUGUSTINOV, G. y DUFTSCHMID, G., "Can the Austrian nation-wide EHR system support the recruitment of trial patients?", *Studies in Health Technology and Informatics*, Núm. 259, 2019

- AUSLOOS, J., "The Right to be Forgotten, a Worth remembering?", *Computer Law & Security Review*, Vol. 28, Núm. 2, 2012

- BAIXAULI FERNÁNDEZ, V. J., y ABELLAN-GARCÍA SÁNCHEZ, F., "El consentimiento y el tratamiento de los datos sanitarios del paciente en la prestación y realización de estudios de investigación de servicios profesionales farmacéuticos asistenciales", *Farmacéuticos comunitarios*, Vol.11, Núm. 1, 2019

- BARCELÓ DOMÉNECH, J., "Consentimiento informado y responsabilidad médica", *Actualidad Jurídica Iberoamericana*, Núm. 8, 2018

- BELTRÁN AGUIRRE, J.L. "Reglamento General de Protección de Datos: Novedades. Adaptación de la normativa española: el proyecto de LOPD", *Derecho y salud*, Vol.28, Núm. 1, 2018

- BHARDWAJ, R.; NAMBIAR, A.R.; DUTTA, D., "A study of machine learning in healthcare". *IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, 2017, https://doi.org/10.1109/COMPSAC.2017.164

- BOECK JENSEN, A.; MOSELEY, P.L.; OPREA, T.I.; GADE ELLESØE, S.; ERIKSSON, R.; SCHMOCK, H.; BJØDSTRUP JENSEN, P.; JUHL JENSEN, L. y BRUNAK, S., "Temporal disease trajectories condensed from population-wide registry data covering 6.2 million patients", *Nature communications*, Vol. 5, Núm. 4022, 2014

- BOURASSA FORCIER, M.; GALLOIS, H.; MULLAN, S. y JOLY, Y., "Integrating artificial intelligence into health care through data access: can the GDPR act as a beacon for policymakers?", *Journal of Law and the Biosciences*, Vol. 6, Núm. 1, 2019

- BUSCA, N., "Il trattamento dei dati sanitari nell´ambito della ricerca e della sperimentazione clínica", *Rivista responsabilita medica*, Núm. 9, 2020

- CABRA DE LUNA, M.A., "La Reforma del Derecho Civil a la luz de la Convención de Nueva York: el rol de la Comisión de Legislación del Real Patronato sobre Discapacidad", *Revista Española de Discapacidad*, Vol. 9, Núm. 2, 2021

- CÁMARA LAPUENTE, S., "La sucesión mortis causa en el patrimonio digital", *Anales de la Academia Matritense del Notariado*, Núm. 59, 2019

- CARABANTES, M., "Black-box artificial intelligence: an epistemological and critical analysis", *AI & society*, 2020, Vol. 35, Núm. 2

- CARBAJO VÉLEZ, M.C., "Mitos y estereotipos sobre la vejez. Propuesta de una concepción realista y tolerante", *Ensayos*, Núm. 24, 2009

- CARVALHO, A. C.; MARTINS, R. y ANTUNES, L., "How-to express explicit and auditable consent", *IEEE*, 2018, disponible en**:** 10.1109/PST.2018.8514204

- CASARES MARCOS, A. B., "Derecho al olvido en internet y autodeterminación informativa personal: el olvido está lleno de memoria", *Revista de administración pública*, núm. 212, 2020

- CASONATO, C., FASAN, M. y PENASA, S., "Diritto e intelligenza artificiale", *DPCE online*, Núm. 1, 2022

- CAVOUKIAN, A., "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian", D. *Identity in the Information Society*, Vol. 3, Núm. 2, 2010

- CAVOUKIAN, A.; FISCHER, A.; KILLEN, S. y HOFFMAN, D.A., "Remote home health care technologies: How to ensure privacy? Build it in: Privacy by design", *Identity in the Information Society*, Vol. 3, Núm. 2, 2010

- CHEW, S.Y; S KOH, M.; MIN LOO, C.; THUMBOO, J.; SHANTAKUMAR, S. y MATCHAR, D. "Making clinical practice guidelines pragmatic: how big data and real world evidence can close the gap", *Ann Acad Med Singapore*, Vol. 47, Núm. 12, 2018

- CLARKE, N.; VALE, G.; REEVES, E.P; KIRWAN, M.; FARRELL, M.; HURL, G. y MCELVANEY, N. G., "GDPR: an impediment to research?", *Irish Journal of Medical Science (1971-)*, Vol. 188, Núm. 4, 2019

- COMANDE,G. y SCHNEIDER,G., "Regulatory Challenges of Data Mining Practices: The Case of the Never-ending Lifecycles of Health Data", *European Journal of Health Law*, Vol. 25, Núm. 3, 2017

- CONNER, J., "Digital life after death: The issue of planning for a person's digital assets after death", *Texas Tech Law School Research Paper*, Núm. 10, 2010

- CONWAY, H. y GRATTAN, S., "The "New" Property: Dealing with Digital Assets on Death", Modern Studies in Property Law, vol. 9, 2017

- CORVALÁN, J., "Inteligencia Artificial y derechos humanos", *Diario DPI Cuántico*, Núm. 1, 2017

- COTINO HUESO, L., "Big data e inteligencia artificial. Una aproximación a su tratamiento jurídico desde los derechos fundamentales", *Dilemata. Revista Internacional de Éticas Aplicadas*, Núm. 24, 2017

- CUENCA GÓMEZ, P., "El sistema de apoyo en la toma de decisiones desde la Convención Internacional sobre los Derechos de las Personas con Discapacidad: principios generales, aspectos centrales e implementación en la legislación española", *Redur*, Núm. 10, 2012

- CUENCA GÓMEZ, P., "Reflexiones sobre el Anteproyecto de reforma de la legislación civil española en materia de capacidad jurídica de las personas con discapacida", *Indret*, Núm. 2, 2020

- CUESTA, J.L.; DE LA FUENTE, R. y ORTEGA, T., "Discapacidad intelectual: una interpretación en el marco del modelo social de la discapacidad", *Controversias y Concurrencias Latinoamericanas*, Vol. 10, Núm. 18, 2019

- DAVEY, M. G.; O'DONNELL, J.P.M.; MAHER, E.; MCMENAMIN, C.; MCANENA, P.F.; KERIN, M. J.; MILLER, N.; Y LOVERY, A. J., "General data protection regulations (2018) and clinical research: perspectives of patients and doctors in an Irish university teaching hospital", *Irish Journal of Medical Science (1971-)*, Vol. 191, Núm. 4, 2021

- DE LA MATA BARRANCO, N.J. y BARINAS UBIÑAS, D., "La privacidad en el diseño y el diseño de la privacidad, también desde el derecho penal", *Eguzkilore*, Núm. 28, 2014

- DE LECUONA, I. "Aspectos éticos, legales y sociales del uso de la inteligencia artificial y el Big Data en salud en un contexto de pandemia", *Revista Internacional de Pensamiento Político*, Núm. 15, 2020

- DE RADA ECHEVARRÍA, M.T., "El consentimiento para la vacuna covid de las personas vulnerables", *OTROSÍ.: Revista del Colegio de Abogados de Madrid*, Núm. 8, 2021

- DÍAZ PARDO, G., "Retribución y gastos derivados del ejercicio de la medida de apoyo a la persona con discapacidad. Nuevas perspectivas tras la Ley 8/2021, de 2 de junio, de reforma de la legislación civil y procesal", *Revista de Derecho Civil*, Vol. 9, Núm. 1, 2022

- DOMARADZKI, S.; KHVOSTOVA, M. y PUPOVAC, D., "Karel Vasak's Generations of Rights and the Contemporary Human Rights Discourse. Human Rights Review", Vol. 20, Núm. 4, 2019

- DONNELLY, M. y MCDONAGH, M., "Health research, consent and the GDPR exemption", *European journal of health law,* Vol. 26, Núm.2, 2019

- DOVE, E. S., y CHEN, J., "Should consent for data processing be privileged in health research? A comparative legal analysis", *International Data Privacy Law,* Vol. 10, Núm. 2, 2020

- DOVE, E.S., "The EU general data protection regulation: implications for international scientific research in the digital era", *Journal of Law, Medicine & Ethics,* Vol. 46, Núm. 4, 2018

- EMALDI CIRIÓN, A., "Protección de datos personales en el ámbito sanitario y de investigación biomédica: Una visión europea", *Actualidad Jurídica Iberoamericana*, Núm.14, 2021

- ESCARTÍN IPIÉNS, J.A., "La autocuratela en el Anteproyecto de Ley sobre modificación del Código Civil y otras leyes complementarias en materia de discapacidad»", *Revista de Derecho Civil*, Vol. 5, Núm. 3, 2018

- EYSENBACH, G., "What is e-health?", *Journal of medical Internet research*, Vol. 3, Núm. 2, 2001

- FABBRINI, F. y CELESTE, E., "The right to be forgotten in the digital age: the challenges of data protection beyond borders", *German law journal*, Vol. 21, Núm. S1, 2020

- FERNÁNDEZ ALLER, C., "Algunos retos de la protección de datos en la sociedad del conocimiento: especial detenimiento en la computación en nube (Cloud Computing)", *Revista de derecho UNED*, Núm. 10, 2012

- FERNÁNDEZ DE BUJÁN, A., "Capacidad. discapacidad. incapacidad. Incapacitación", *revista de derecho UNED*, Núm. 9, 2011

- FERNÁNDEZ LÓPEZ, J. M., "El derecho fundamental a la protección de los datos personales. Obligaciones que derivan para el personal sanitario", *Derecho y salud*, Vol. 11, Núm. 1, 2003

- FERNÁNDEZ VILLAZÓN, L. A. "El nuevo reglamento europeo de protección de datos". *Foro. Revista de Ciencias Jurídicas y Sociales, Nueva Época*, Vol. 19, Núm. 1, 2016

- FERRÉ, E.A., "La nueva guarda de hecho como verdadera institución de apoyo", *Revista Boliviana de Derecho*, Núm. 30, 2020

- FLAQUER, L., "La emancipación familiar de los jóvenes", *Revista de estudios de juventud*, Núm. 39, 1997

- FOMBELLA POSADA, M.J. y CEREIJO QUINTEIRO, M.J., "Historia de la historia clínica", *Galicia Clínica*, Vol. 73, Núm.1, 2012

- GALINDO AYUDA, F., "¿Inteligenciaa Artificial y Derecho? Sí, pero ¿cómo?", *Revista Democracia Digital e Governo Eletrônico*, Vol.2, Núm.18, 2019

- GALLEGO RIESTRA, S. y RIAÑO GALÁN, I., "¿Tiene el paciente derecho a saber quiénes y por qué han accedido a su historia clínica?", *Derecho y salud*, Vol. 22, Núm. 1, 2012

- GALLEGO RIESTRA, S., "Historia clínica electrónica y derecho a la autonomía del paciente: Un conflicto de intereses", *Papeles Médicos*, Vol. 23, Núm. 1, 2014

- GÁRATE ITURRI, J.C., "Concepto jurídico de discapacidad", *Anales de derecho y discapacidad*, Núm. 6, 2021

- GARCÍA PÉREZ, R.M., "Bases jurídicas relevantes del tratamiento de datos personales en la contratación de contenidos y servicios digitales", *Cuadernos de derecho transnacional*, Vol. 12, Núm. 1, 2020

- GARCÍA PONS, A., "El artículo 12 de la Convención de Nueva York de 2006 sobre los Derechos de las Personas con Discapacidad y su impacto en el Derecho Civil de los Estados signatarios: el caso de España", *Anuario de derecho civil*, Vol. 66, Núm. 1, 2013

- GARCÍA RUBIO, M.P., "Las medidas de apoyo de carácter voluntario, preventivo o anticipatorio", *Revista de Derecho Civil*, Vol. 5, Núm. 3, 2018

- GHAFUR, S.; KRISTENSEN, S.; HONEYFORD, K.; MARTIN, G.; DARZI, A. y AYLIN, P., "A retrospective impact analysis of the WannaCry cyberattack on the NHS", *NPJ digital medicine*, Vol. 2, Núm. 1, 2019

- GIANNOPOULOU, A., "Algorithmic systems: the consent is in the detail?", *Internet Policy Review*, Vol. 9, Núm. 1, 2020

- GIL RODRÍGUEZ, J., "La tutela como garantía de las personas incapacitadas y del respeto de sus derechos", *Revista del poder judicial*, Núm. 81, 2006

- GINEBRA MOLINS, M.E., "Voluntades digitales en caso de muerte", *Cuadernos de derecho transnacional*, Vol. 12, Núm. 1, 2020

- GÓMEZ, J.E., "El internet de las cosas oportunidades y desafíos", *Ingeniería e Innovación*, Vol. 5, Núm. 1, 2017

- GÓMEZ-JUAREZ SIDERA, I., "Hacia un nuevo derecho de protección de datos para las personas especialmente vulnerables en la sociedad digital del siglo XXI: los niños y las personas mayores", *Revista CESCO de Derecho de Consumo*, Núm. 4,2015

- GONZÁLEZ CARRASCO, C., "La prestación del consentimiento informado en materia de salud en el nuevo sistema de apoyos al ejercicio de la capacidad", *Derecho privado y Constitución*, Núm. 39, 2021

- GONZÁLEZ OÑATE, C. y FANJUL PEYRÓ, C., "Aplicaciones móviles para personas mayores: un estudio sobre su estrategia actual", *Aula abierta*, Vol. 47, Núm. 1, 2018

- GONZÁLEZ OÑATE, C.; FANJUL PEYRÓ, C. y CABEZUELO LORENZO, F., "Uso consumo y conocimiento de las nuevas tecnologías en personas mayores en Francia, Reino Unido y España", *Comunicar,* Núm.45, 2015

- GRASSELLI, F. y TEVERE, V., "Il green pass esteso nello spazio europeo multilevel di libertà, sicurezza e giustizia. Riglessioni sull´eventuale introduzione dell´obbligatorietà vaccinale", *Freedom, Sevurity & Justice: European Legal Studies,* Núm.3, 2021

- GUILARTE MARTÍN-CALERO, C., "Algunas consideraciones sobre el consentimiento de las personas con discapacidad mental e intelectual", *Revista Doctrinal Aranzadi Civil-Mercantil*, Núm. 11, 2018

- GUILLÉN CATALÁN, R., "Sujetos responsables por vulneración de las normas de protección de datos. Especial referencia a los datos relativos a la salud", ***Revista Boliviana de Derecho,*** Núm. 30, 2020

- HERNANDO, P.; SEOANE, J.A. y DE ASÍS, J.F., "La reserva de las anotaciones subjetivas: ¿derecho o privilegio?", *Revista de calidad asistencial*, Vol. 21, Núm. 1, 2006

- HERRÁN ORTIZ, A.I., "El derecho a la protección de datos personales en la sociedad de información", *Cuadernos Deusto de Derechos Humanos,* Núm. 26, 2003

- HILDEBRANDT, M., "Slaves to big data. Or are we?", IDP *Revista de Internet, Derecho y Política*, núm. 17, 2013

- HUMMEL, P; BRAUN, M y DABROCK, P., "Data Donations as Exercises of Sovereignty", En: KRUTZINA, J y FLORIDI, L., *The ethics of medical data donation*, Springer, 2019

- IMAZ ZUBIAUR, L., "Reformulando la protección de las personas con diversidad funcional a la luz de la distante Convención de Nueva York de 2006", *Revista Vasca de Administración Pública,* Núm. 112, 2018

- JAUREGUI, J.R. y RUBIN, R.K., "Fragilidad en el adulto mayor", *Revista del hospital italiano de Buenos Aires*, Vol. 32, Núm. 3, 2012

- JERVIS ORTIZ, P., "Internet de las cosas y protección de datos personales", *Revista Chilena de Derecho y Tecnología*, Vol. 4, Núm. 2, 2015

- KIVE, M. y GRASIS, J., "Problems of application of the right to data portability", *Acta Prosperitatis,* Núm.11, 2020

- LECIÑENA IBARRA, A., "Reflexiones sobre la formación de la voluntad negocial en personas que precisan apoyos en el ejercicio de su capacidad jurídica", *Revista de Derecho Civil,* Vol. 9, Núm. 1, 2022

- LETURIA INFANTE, F.J., "Fundamentos jurídicos del derecho al olvido: ¿un nuevo derecho de origen europeo o una respuesta típica ante colisiones entre ciertos fundamentos?", *Revista chilena de derecho,* Vol. 43, Núm. 1, 2016

- LINARES GUTIÉRREZA, A., "El consentimiento en los contratos telefónicos de prestación de servicios de comunicaciones ante la nueva regulación sobre protección de datos personales", *Revista Internacional Jurídica y Empresarial,* Núm. 2, 2019

- LOHAR, P.; XIE, G.; BENDECHACHE, M.; BRENNAN, R.; CELESTE, E.; TRESTIAN, R. y TAL, I., "Irish attitudes toward COVID tracker app & privacy: sentiment analysis on Twitter and survey data", *The 16th International Conference on Availability, Reliability and Security*, Núm.37, 2021

- LÓPEZ DE MÁNTARAS, R., "Algunas reflexiones sobre el presente y futuro de la Inteligencia Artificial", *Novática,* Núm. 234, 2015

- LÓPEZ SAN LUIS, R., "El principio de respeto a la voluntad de la persona con discapacidad en la Convención de Nueva York y su reflejo en el anteproyecto por la que se reforma la legislación civil y procesal en materia de discapacidad", *InDret*, Núm. 2, 2020

- MACÍAS GONZÁLEZ, L. y MANRESA YEE, C., "Mayores y nuevas tecnologías: motivaciones y dificultades", *Ariadna: cultura, educación y tecnología*, Vol. 1, Núm. 1, 2013

- MAHESH, B., "Machine learning algorithms-a review", *International Journal of Science and Research,* Vol. 9, Núm, 2020

- MALGIERI, G., "Data Protection and Research: A vital challenge in the era of Covid-19 Pandemic", *Computer Law & Security Review,* Núm. 37, 2020

- MARTÍNEZ DEL VALLE, M., "Covid-19: más que una pandemia, un cambio en nuestra consulta", *Medicina general y de familia*, Vol. 9, Núm. 4, 2020

- MARTÍNEZ HERNÁNDEZ, J., "Historia clínica", *Cuadernos de bioética,* Vol. 17, Núm. 1, 2006

- MARTÍNEZ MARTÍNEZ, N., "Reflexiones en torno a la protección post mortem de los datos personales y la gestión de la transmisión mortis causa del patrimonio

digital tras la aprobación de la LOPDGDD", *Derecho Privado y Constitución*, Núm. 35, 2019

- MARTÍNEZ OTERO, J.M., "El derecho al olvido en internet: debates cerrados y cuestiones abiertas tras la STJUE Google vs AEPD y Mario Costeja", *Revista de derecho político*, Núm. 93, 2015

- MARTÍNEZ ROLÁN, X. y PIÑERO OTERO, T., "Tipología y funcionalidades de las aplicaciones móviles para mayores. A un tap del envejecimiento activo", *Ámbitos Revista Internacional de Comunicación*, Núm. 29, 2015

- MARTÍNEZ-PUJALTE, A.L., "A propósito de la reforma de la legislación española en materia de capacidad jurídica: la voluntariedad como nota esencial del apoyo", *Cuadernos Electrónicos de Filosofía del Derecho*, Núm.42, 2020

- MATÍNEZ RAMOS, C., "Las TIC en la Hospitalización y en la Atención Domiciliarias", *Reduca*, Vol. 1, Núm. 1, 2009

- MEE, B.; KIRWAN, M.; CLARKE, N.; TANAKA, A.; MANALOTO, L.; HALPIN, E.; GIBBONS,U.; CULLEN, A.; MCGARRIGLE, S.; CONNOLLY, E.; BENNETT, K.; GAFFNEY, E.; TIER, L.; FLAVIN, R. y MCELVANEY, N.G., "What GDPR and the Health Research Regulations (HRRs) mean for Ireland: a research perspective", *Irish Journal of Medical Science (1971-)*, Vol. 190, Núm.2, 2020

- MÉNDEZ GARCÍA, M. y ALFONSO FARNÓS, I., "La legitimación para el tratamiento de categorías especiales de datos con finalidades de investigación en el marco del Reglamento (UE) 2016/679 y de la Ley Orgánica 3/2018", *Revista de derecho y genoma humano*, Vol. 205, Núm. 231, 2019

- MESTRE GONZÁLEZ, A., "La autonomía del paciente con enfermedades crónicas: De paciente pasivo a paciente activo", *Enfermería clínica*, Vol. 24, Núm. 1, 2014

- MÉSZÁROS, J. y HO, C. H. "Big data and scientific research: the secondary use of personal data under the research exemption in the GDPR". *Hungarian Journal of Legal Studies*, Vol. 59, Núm. 4, 2018

- MÉSZÁROS, J., "The Conflict Between Privacy and Scientific Research in the GDPR", IEEE, 2018, disponible en: 10.23919/PNC.2018.8579471

- MEYSTRE, S., "The current state of telemonitoring: a comment on the literature", *Telemedicine Journal & e-Health*, Vol. 11, Núm. 1, 2005

- MICOZZI, F. P., "Le tecnologie, la protezione dei dati e l'emergenza Coronavirus: rapporto tra il possibile e il legalmente consentito", *BioLaw Journal-Rivista di BioDiritto*, Núm especial. 1, 2020

- MITTAL, S. y SHARMA, P., "The role of consent in legitimising the processing of personal data under the current EU data protection framework", *Asian Journal of Computer Science And Information Technology*, Vol. 7, Núm. 4, 2017

- MOEREL, L. y PRINS, C., "Privacy for the Homo Digitalis: Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things", *Tilburg University*, 2016, disponible en: http://dx.doi.org/10.2139/ssrn.2784123

- MOHURLE, S. y PATIL, M., "A brief study of wannacry threat: Ransomware attack 2017", *International Journal of Advanced Research in Computer Science*, Vol. 8, Núm. 5, 2017

- MOJICA LOPEZ, M.; RODRIGO OLIVA, J.L.; GAYOSO MARTÍNEZ, V.; HERNANDEZ ENCINAS, L. y MARTÍN MUÑOZ, A., "Análisis de la privacidad de WhatsApp Messenger", *Revista de sistemas, cibernética e informática*, Vol. 14, Núm. 2, 2017

- MONTEAGUDO, J.L.; SERRANO, L. y HERNÁNDEZ SALVADOR, C., "La telemedicina: ¿ciencia o ficción?", *Anales del sistema sanitario de Navarra*, Vol. 28, Núm.3, 2005

- MONTERO MARTÍNEZ, M.A., "Retos y oportunidades del Cloud Computing en la sanidad", *Revista Informática y Salud* (I+S), Núm. 88, 2011

- MORALEJO IMBERNÓN, N., "El testamento digital en la nueva Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales", *Anuario de derecho civil*, 2020, disponible en: https://www.boe.es/biblioteca_juridica/anuarios_derecho/abrir_pdf.php?id=ANU-C-2020-10024100281

- MORENO RODRÍGUEZ, M.D., "Alfabetización digital: el pleno dominio del lápiz y el ratón", *Comunicar*, Vol. 15, Núm. 30, 2008

- MORENO MORENO, J., "Mayores y calidad de vida", *Portularia*, Núm. 4, 2004

- MORENO TOLEDO, A., "La cuarta edad. Perfil conceptual de la vejez avanzada", *Poiésis*, Vol. 10, Núm. 20, 2010

- MORSE, T. y BIRNHACK, M., "The posthumous privacy paradox: Privacy preferences and behavior regarding digital remains", *New Media & Society,* Vol. 24, Núm. 6, 2022

- MUNAR BERNAT, P., "A. La curatela: Principal medida de apoyo de origen judicial para las personas con discapacidad", *Revista de Derecho civil*, Vol. 5, Núm. 3, 2018

- MURILLO DE LA CUEVA, P., "El derecho a la autodeterminación informativa y la protección de datos personales", *Azpilcueta*, Núm. 20, 2008

- NICOLÁS, P., "Los derechos sobre los datos utilizados con fines de investigación biomédica ante los nuevos escenarios tecnológicos y científicos", *Revista de Derecho y Genoma Humano*, Núm. extraordinario, 2019

- NIÑO GONZÁLEZ, J.I. y FERNÁNDEZ MORALES, B., "Comunicación, Salud y tecnología: mHealth", *Revista de comunicación y salud*, Vol. 5, 2015

- NOAIN-SÁNCHEZ, A., "Privacy by default and active informed consent by layers: Essential measures to protect ICT users' privacy", *Journal of Information, Communication and Ethics in Society,* Vol.14, Núm.2, 2016

- ORDELIN FONT, J.L. y ORO BOFF, S., "Bienes digitales personales y sucesión mortis causa: la regulación del testamento digital en el ordenamiento jurídico español", *Revista de derecho (Valdivia),* Vol. 33, Núm. 1, 2020

- PÁEZ MORENO, R., "La riqueza del principio de no maleficencia", *Cirujano General*, 2011, Vol. 33, Núm. S2, 2011

- PAU PEDRÓN, A., "De la incapacitación al apoyo: el nuevo régimen de la discapacidad intelectual en el Código Civil", *Revista de Derecho Civil*, Vol. 5, Núm. 3, 2018

- PAU PEDRÓN, A., "El principio de igualdad y el principio de cuidado, con especial atención a la discapacidad", *Revista de Derecho Civil*, Vol. 7, Núm. 1, 2020

- PAU PEDRÓN, A., "La reforma de las instituciones de protección", *OTROSÍ: Revista del Colegio de Abogados de Madrid*, Núm. 8, 2021

- PELOQUIN, D.; DIMAIO, M.; BIERE, B. y BARNES, M., "Disruptive and avoidable: GDPR challenges to secondary research uses of data", *European Journal of Human Genetics,* Vol. 28, Núm. 6, 2020

- PEREA MARTÍN, P., "Cloud Computing contribuye a la sostenibilidad del sistema sanitario", *Revista Informática y Salud (I+S)*, Núm. 88, 2011

- PEREÑA VICENTE, M., "La transformación de la guarda de hecho en el Anteproyecto de Ley", *Revista de Derecho Civil*, Vol. 5, Núm. 3, 2018

- POLO ROCA, A., "El derecho a la protección de datos personales y su reflejo en el consentimiento del interesado", *Revista de Derecho Político*, Vol. 1, Núm. 108, 2020

- PRENSKY, M., "Digital natives, digital immigrants. On the horizon", *MCB university press*, Vol. 9, Núm. 5, 2001

- PUCCINELLI, O.R., "El derecho a la portabilidad de los datos personales. Orígenes, sentido y alcances", *Pensamiento constitucional*, Vol. 22, Núm. 22, 2017

- PUYOL, J., "Una aproximación a big data", *Revista de Derecho de la Universidad Nacional de Educación a Distancia (UNED)*, Núm.14, 2014

- QUIGLEY, E.; HOLME, I.; DOYLE, D. M.; HO, A. K.; AMBROSE, E.; KIRKWOOD, K. y DOYLE, G., "Data is the new oil: citizen science and informed consent in an era of researchers handling of an economically valuable resource", *Life Sciences, Society and Policy*, Vol. 17, Núm. 1, 2021

- RODRÍGUEZ AYUSO, J.F., "Dossier cuestiones bioéticas de la pandemia covid-19", *Revista de Bioética y Derecho*, Núm. 50, 2020

- RODRÍGUEZ AYUSO, J.F., "Estado de alarma y protección de la privacidad en tiempos de pandemia: licitud del tratamiento de categorías especiales de datos", *Revista De Derecho Político*, Núm. 110, 2021

- ROMANOU, A., "The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise", *Computer law & security review*, Vol. 34, Núm. 1, 2018

- ROMERO CARBERA, A.R., "Fragilidad: un síndrome geriátrico emergente", *Medisur*, Vol. 8, Núm. 6, 2010

- RONCATI, L. y RONCATI, M., "COVID-19 Green Pass: a Lesson on the Proportionality Principle from Galicia", *European Journal of Health Law*, Núm. 1, 2021

- RUBÍ NAVARRETE, J., "La protección de datos personales en la pandemia de COVID-19", *Comunicaciones en propiedad industrial y derecho de la competencia*, Núm. 90, 2020

- RUDA GONZÁLEZ, A. "Sé lo que hicisteis el último verano. Implicaciones ético-jurídicas del programa de Big Data de Salud en Cataluña a la luz del Reglamento Europeo de Protección de datos", *Papeles el tiempo de los derechos*, Núm. 29, 2018

- RUFO, L., "Le ricerche scientifiche durante l'emergenza sanitaria (il covid-19). Quale base giuridica per l'arruolamento dei pazienti", *BioLaw Journal-Rivista di BioDiritto*, Núm especial. 1, 2020

- RUMBOLD, J. M. M., y PIERSCIONEK, B., "The effect of the general data protection regulation on medical research", *Journal of medical Internet research*, Vol. 19, Núm. 2, 2017

- SAINZ DE ABAJO, B., "M-health y T-health. La evolución natural del E-health", *RevistaeSalud. com*, Vol. 7, Núm. 25, 2011

- SÁIZ RAMOS, M. y LARIOS RISCO, D., "El derecho de acceso a la historia clínica por el paciente: propuesta para la reserva de anotaciones subjetivas", *Derecho y salud*, Vol. 18, Núm. 1, 2009

- SALDAÑA, M.N., "The right to privacy: la génesis de la protección de la privacidad en el sistema constitucional norteamericano, el centenario legado de Warren y Brandeis", *Revista de Derecho Político*, Núm. 85, 2012

- SALIDO, J.; DÉNIZ, O. Y BUENO, G., **"**Especial m-health (salud móvil): Desarrollo de aplicaciones de salud para dispositivos móviles", *Sociedad Española de Informática y Salud*, Núm.110, 2015

- SALUD CASANOVA ASENCIO, A., "Protección de datos en el ámbito de la historia clínica: el acceso indebido por el personal sanitario y sus consecuencias", *Indret*, Núm.2, 2019

- SÁNCHEZ CARAZO, C., "La protección de datos personales de las personas vulnerables", *Anuario de la Facultad de Derecho de la Universidad de Alcalá II*, Núm. 2, 2009

- SÁNCHEZ HERNÁNDEZ, A., "Aspectos generales de la reforma del Código civil relativa a las personas con discapacidad intelectual en el ejercicio de su capacidad jurídica", *Revista Boliviana de Derecho*, Núm. 33, 2022

- SÁNCHEZ HERNÁNDEZ, A., "Consideraciones sobre la reforma de la legislación civil en materia de discapacidad: de la incapacitación al apoyo", *Redur*, Núm. 19, 2021

- SÁNCHEZ HERNÁNDEZ, A., "La guarda de apoyo: propuesta para la protección de la persona mayor con discapacidad", *Revista jurídica de Castilla y León*, Núm. 44, 2018

- SANDBERG, L., "Affirmative old age- The ageing body and feminist theories on difference", *International Journal of Ageing and Later Life*, Vol.8, Núm.1, 2013

- SANTOS DIVINO, S.B., "Reflexiones escépticas, principiológicas y económicas sobre el consentimiento necesario para la recolección y tratamiento de datos", *Derecho PUCP*, Núm. 83, 2019

- SANTOS MORÓN, M.J., "La denominada "herencia digital": ¿necesidad de regulación? Estudio de Derecho español y comparado", *Cuadernos de Derecho transnacional*, Vol.10, Núm.1, 2018

- SARRATO MARTÍNEZ, L., "El régimen legal de acceso a la historia clínica y sus garantías", *revista jurídica de castilla y león*, Núm. 17, 2009

- SCHAAR, P., "Privacy by design", *Identity in the Information Society*, Vol. 3, Núm. 2, 2010

- SCHERMER, B.W.; CUSTERS, B.; VAN DER HOF, S., "The crisis of consent: How stronger legal protection may lead to weaker consent in data protection", *Ethics and Information Technology*, Vol. 16, Núm. 2, 2014

- SERRANO PÉREZ, M. M., "El marco jurídico de los datos relativos a la salud en el ámbito de la salud y de la investigación en salud tras la entrada en vigor del Reglamento General de Protección de Datos y de la Ley de Protección de Datos Personales y garantía de los derechos", *Estudios de Deusto*, Vol. 68, Núm. 2, 2020

- SHABANI, M., "The Data Governance Act and the EU's move towards facilitating data sharing", *Molecular Systems Biology*, Vol. 17, Núm.3, 2021

- SHEEHY, A.; JAMES, J.R.; HORGAN, M., "Implementing a National Approach to Research Ethics Review during a Pandemic-the Irish Experience", *HRB Open Research*, 2020, doi:10.12688/hcbopenres.12146.1

- SHEFET, D., "The right to be forgotten", *Scitech Lawyer*, Vol. 16, Núm. 3, 2020

- SOMAINI, L., "The right to data portability and user control: ambitions and limitations", *Rivista di diritto dei media*, Núm. 3, 2018

- SORIANO ARNANZ, A., "Decisiones automatizadas: problemas y soluciones jurídicas. Más allá de la protección de datos", *Revista de derecho público: teoría y método*, Vol. 3, 2021

- STOYKOVA, R., "The right to data portability as a market tool", *Computer Law Review International*, Vol. 19, Núm. 2, 2018

- TIKKINEN-PIRI, C.; ROHUNEN, A. y MARKKULA, J., "EU General Data Protection Regulation: Changes and implications for personal data collecting companies", *Computer Law & Security Review*, Vol. 34, Núm. 1, 2018

- TIRADO, F.; LÓPEZ, D., CALLÉN, B. y DOMÈNECH, M., "La producción de fiabilidad en entornos altamente tecnificados. Apuntes etnográficos sobre un servicio de teleasistencia domiciliaria", *Papeles del CEIC*, Vol. 2, Núm. 38, 2008

- TORTAJADA CHARTÍ, P., "La patria potestad prorrogada y la patria potestad rehabilitada en el nuevo proyecto de Ley de reformas de la legislación civil y procesal para el apoyo a las personas con discapacidad (actual Ley 8/2021)", *Revista Boliviana de Derecho*, Núm. 32, 2021

- TOYGAR, A.; TAPIE, C.E.; ZHU, J., "A new asset type: digital assets", *Journal of International Technology and Information Management*, Vol. 22, Núm. 4, 2013

- TRESTIAN, R.; XIE, G.; LOHAR, P.; CELESTE, E.; JAYASEKERA, E.; CONNOLLY, R. y TAL, I., "Privacy in a Time of COVID-19: How Concerned Are You?", *IEEE Security & Privacy*, vol. 19, Núm. 5, 2021

- TRIGO VILASECA, J.D.; SERRANO-ARRIEZU, L.; ASTRAIN ESCOLA, J.J; FALCONE LANAS, F., "Smart Cities, IoT y Salud: Retos de Internet of Medical Things (IoMT)", *I+ S: Revista de la Sociedad Española de Informática y Salud*, Núm. 129, 2018

- TROCHIM, W.; KANE, C.; GRAHAM, M.J. y PINCUS, H.A., "Evaluating translational research: a process marker model", *Clinical and translational science*, Vol. 4, Núm. 3, 2011

- TRONCOSO REIGADA, A., "La confidencialidad de la historia clínica", *Cuadernos de derecho público*, Núm. 27, 2006

- TURNER, S.; GALINDO QUINTERO, J.; TURNER, S.; LIS, J.; TANCZER, L.M., "The Exercisability of the Right to Data Portability in the Emerging Internet of Things (Iot) Environment", *New Media & Society*, Vol. 23, Núm.10, 2020

- URQUHART, L.; SAILAJA, N.; MCAULEY, D., "Realising the Right to Data Portability for the Domestic Internet of Things", *Personal and Ubiquitous Computing*, Vol. 22, Núm. 2, 2018

- VAN DER AUWERMEULEN, B., "How to attribute the right to data portability in Europe: A comparative analysis of legislations", *Computer law & security review*, Vol. 33, Núm.1, 2017

- VAN DER SLOOT, B. Y VAN SCHENDEL, S., "Ten Questions for the Future Regulation of Big Data: A Comparative and Empirical Legal Study", *JIPITEC: Journal of Intellectual Property, Information Technology and E-Commerce Law*, Vol. 7, 2016

- VILLALOBOS-QUESADA, M., "Participative consent: Beyond broad and dynamic consent for health big data resources", *Revista de derecho y genoma humano*, Núm. Extra 1, 2019

- VILLARES, D.J., "Datos relativos a la salud y datos genéticos: consecuencias jurídicas de su conceptualización". *Revista Derecho y Salud Universidad Blas Pascal*, Núm. 1, Vol. 1, 2017

- VIVAS-TESÓN, I., "Autodeterminación informativa, validez del consentimiento y protección de datos sensibles: críticas al nuevo marco normativo", *Revista de Derecho y genoma humano*, Núm. Extraordinário, 2019

- VIVAS-TESÓN, I., "Discapacidad y consentimiento informado en el ámbito sanitario y bioinvestigador", *Pensar-Revista de Ciências Jurídicas*, Vol. 21, Núm. 2, 2016

- VIVAS-TESÓN, I., "Discapacidad y consentimiento informado en materia de tratamientos sanitarios y de bioinvestigación", *Civilistica. com*, Vol. 3, Núm. 2, 2014

- VIVAS-TESÓN, I., "El consentimiento del adulto frágil al tratamiento de muestras biológicas y datos genéticos con fines de investigación biomédica: comparación entre el derecho español e italiano. Revista de derecho y genoma humano", Núm. 40, 2014

- VIVAS-TESÓN, I., "Retos actuales en la protección jurídica de la discapacidad", *Pensar-Revista de Ciências Jurídicas*, Vol. 20, Núm. 3, 2015

- WACHTER, S.; MITTELSTADT, B.; FLORIDI, L., "Why a right to explanation of automated decision-making does not exist in the general data protection regulation", *International Data Privacy Law*, Vol. 7, Núm. 2, 2017

- WAITZBERG, R.; TRIKI, N.; ALROY-PREIS, S.; LOTAN, T.; SHIRAN, L. y ASH, N., "The Israeli Experience with the "Green Pass" Policy Highlights Issues to Be Considered by Policymakers in Other Countries", *International Journal of Environmental Research and Public Health*, Vol. 18, Núm. 21, 2021

- WALLACE, R. y GREENE, E., "Survey of NCHDs in Ireland to assess their views and opinions in relation to participation in health research and the impact of new Irish data protection regulations", *Irish Journal of Medical Science*, Vol. 189, Núm. 3, 2020

- WALSH, B.; MAC DOMHNAILL, C. y MOHAN, G., "Developments in healthcare information systems in Ireland and internationally", *ESRI survey and statistical series*, Núm.105, 2021

- WARREN, S.D. y BRANDEIS, L.D. "The right to privacy", *Harvard law review*, Vol.4, Núm.5, 1890

- WEGLARZ, G., "Two worlds of data unstructured and structured", *Information Management*, Vol. 14, Núm. 9, 2004

- WENDLER, D., "Broad versus Blanket Consent for Research with Human Biological Samples", Hasting center report, Vol. 43, Núm. 5, 2013

- WONG, J. y HENDERSON, T., "The right to data portability in practice: exploring the implications of the technologically neutral GDPR", *International Data Privacy Law*, Vol. 9, Núm. 3, 2019

- ZURITA MARTÍN, I., "La esperada y necesaria reforma del Código Civil en materia de personas con discapacidad", *Revista de Estudios Jurídicos y Criminológicos*, Núm. 3, 2021

- **RECURSOS ELECTRÓNICOS:**

- ABOGACÍA ESPAÑOLA., "El Consejo de la UE aprueba el Reglamento de Gobernanza de Datos", *abogacía*, 17 de mayo de 2022, disponible en: https://www.abogacia.es/actualidad/noticias/el-consejo-de-la-ue-aprueba-el-reglamento-de-gobernanza-de-datos/

- AEM., "COVID-19 vaccines", *ema.europa.eu*, disponible en: https://www.ema.europa.eu/en/human-regulatory/overview/public-health-threats/coronavirus-disease-covid-19/treatments-vaccines/covid-19-vaccines https://hayderecho.expansion.com/2020/04/10/el-interes-publico-de-los-datos-personales-en-tiempos-del-covid-19/

- AEPD., "Principios", *aepd*, 30 de agosto de 2019, disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/principios#:~:text=Principio%20de%20%E2%80%9C%20limitaci%C3%B3n%20de%20la,leg%C3%ADtimos%20sean%20tratados%20posteriormente%20de

- AEPD. ,"¿Pueden acceder los padres a las historias clínicas de sus hijos mayores de 14 años?", *aepd*, disponible en: https://www.aepd.es/es/preguntas-frecuentes/10-menores-y-educacion/FAQ-1005-pueden-acceder-los-padres-a-las-historias-clinicas-de-sus-hijos-mayores-de-14

- AEPD., "ANEXO WP242 – Preguntas más frecuentes", *aepd*, disponible en: https://www.aepd.es/sites/default/files/2019-09/wp242rev01-annex-es.pdf

- AEPD., "Comunicado en relación con webs y apps que ofrecen autoevaluaciones y consejos sobre el Coronavirus", 16 de marzo de 2020, disponible en: https://www.aepd.es/es/prensa-y-comunicacion/notas-de-prensa/comunicado-de-la-aepd-en-relacion-con-webs-y-apps-que-ofrecen

- AEPD., "Derecho a no ser objeto de decisiones individuales automatizadas", *aepd*, 14 de junio de 2022, disponible en: https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos/derecho-no-ser-objeto-de-decisiones-individuales

- AEPD., "El deber de informar y otras medidas de responsabilidad proactiva en apps para dispositivos móviles", *aepd*, 17 de septiembre de 2019, disponible en: https://www.aepd.es/sites/default/files/2019-11/nota-tecnica-apps-moviles.pdf

- AEPD., "Formulario del derecho a no ser objeto de decisiones individuales automatizadas", *aepd*, disponible en: https://www.aepd.es/es/documento/formulario-derecho-de-oposicion-decisiones-automatizadas.pdf

- AEPD., "Formulario del derecho de acceso", *aepd*, disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-acceso.pdf

- AEPD., "Formulario del derecho de la portabilidad", *aepd*, disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-portabilidad.pdf

- AEPD., "Formulario del derecho de limitación del tratamiento", *aepd*, disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-limitacion.pdf

- AEPD., "Formulario del derecho de oposición", *aepd*, disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-oposicion.pdf

- AEPD., "Formulario del derecho de rectificación", *aepd*, disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-rectificacion.pdf

- AEPD., "Formulario del derecho de supresión", *aepd*, disponible en: https://www.aepd.es/sites/default/files/2019-09/formulario-derecho-de-supresion.pdf

- AEPD., "Guía sobre el uso de las cookies", *aepd*, julio del 2020, disponible en: https://www.aepd.es/sites/default/files/2020-07/guia-cookies.pdf

- AEPD., "Informe sobre políticas de privacidad en internet", *aepd*, septiembre de 2018, disponible en: https://www.aepd.es/sites/default/files/2019-09/informe-politicas-de-privacidad-adaptacion-RGPD.pdf

- AEPD., "Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos (art 35.4)", *aepd*, 4 de septiembre de 2019, disponible en: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-es-35-4.pdf

- AEPD., "Medidas de protección de datos desde el diseño y por defecto", *aepd*, 27 de febrero de 2020, disponible en: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/proteccion-de-datos-diseno-por-defecto

- AEPD., "Recibo del consentimiento: Una herramienta de transparencia y responsabilidad proactiva", *aepd*, 27 de febrero de 2020, disponible en: https://www.aepd.es/es/prensa-y-comunicacion/blog/recibo-del-consentimiento-una-herramienta-de-transparencia-y

- AEPD., Guía para pacientes y usuarios de la sanidad, *aepd*, noviembre 2019, disponible en: https://www.aepd.es/sites/default/files/2019-12/guia-pacientes-usuarios-sanidad.pdf

- ANDRÉS RICART, G., "El consentimiento y el Reglamento de Protección de datos", *legaltoday*, 4 de octubre de 2019, disponible en:

https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/el-consentimiento-y-el-reglamento-de-proteccion-de-datos-2019-10-04/

- APCPD., "Derecho al olvido", *apcpd*, disponible en: https://www.apcpd.es/derecho-al-olvido/

- AVPD., "Mis derechos", *avpd*, disponible en: https://www.avpd.euskadi.eus/s04-5273/es/contenidos/informacion/misderechos/es_def/index.shtml#10

- AYUDA LEY DE PROTECCIÓN DE DATOS., "La seudonimización de los datos y su importancia en el nuevo RGPD", *ayudaleydeprotecciónd atos*, disponible en: https://ayudaleyprotecciondatos.es/2020/11/18/seudonimizacion-de-datos/

- BACH, M. y KERZNER, L., "A New Paradigm for Protecting Autonomy and the Right to Legal Capacity", *lco-cdo*, 2010, disponible en: https://www.lco-cdo.org/wp-content/uploads/2010/11/disabilities-commissioned-paper-bach-kerzner.pdf

- BELTRÁN AGUIRRE, J. L., "La protección de los datos personales relacionados con la salud", *Ponencia presentada en el Defensor del Pueblo de Navarra*, 27 de junio de 2012, disponible en: https://www.navarra.es/NR/rdonlyres/517A4434-9C3B-442E-8651-61A7AE0490AD/226320/pdps.pdf

- BELTRÁN AGUIRRE, J. L.; GARCÍA LÓPEZ, F. J. Y NAVARRO SÁNCHEZ, C., "Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD", *sespas*, noviembre de 2017, disponible en: https://sespas.es/wp-content/uploads/2018/02/SESPAS_informe_proteccion_datos_2017.pdf

- BOLOGNINI, L., "GDPR, come l´Italia minaccia la ricerca scientifica", *agendadigitale*, 6 de diciembre de 2017, disponible en: https://www.agendadigitale.eu/sicurezza/codice-privacy-una-tagliola-italiana-in-contrasto-con-il-gdpr/

- BOZA RUCOSA, M., "Comentario crítico a la Ley 8/2021", *Bozarucosa*, disponible en: https://bozarucosa.com/blog/comentario-critico-a-la-ley-8-2021/

- CABALLERO TRENADO, L., "Primera multa post RGPD en Portugal", *legaltoday*, 29 de noviembre de 2018, disponible en: https://www.legaltoday.com/practica-juridica/derecho-publico/proteccion-datos/primera-multa-post-rgpd-en-portugal-2018-11-29/

- CABANAS TREJO, R., "Observaciones irrespetuosas sobre la Ley 8/2021 para la práctica notarial", *notariosyregistradores*, 8 de septiembre de 2021, disponible en:

https://www.notariosyregistradores.com/web/secciones/oficina-notarial/otros-temas/observaciones-irrespetuosas-sobre-la-ley-8-2021-para-la-practica-notarial/

- CABEZAS VÁZQUEZ, R., "Proteger la privacidad desde el diseño del producto", *Cincodías.elpaís*, 31 de julio de 2019, disponible en: https://cincodias.elpais.com/cincodias/2019/07/30/companias/1564510266_593013.html

- CÁRCAR BENITO, J.E., "El Big Data en la organización sanitaria: nuevos tiempos y nuevos cambios", *Blog Federación Española de Sociología (FES)*, disponible en: https://docplayer.es/41738879-El-big-data-en-la-organizacion-sanitaria-nuevos-tiempos-y-nuevos-cambios-un-estudio-previo.html

- CARRASCO, M., "Fragilidad: Un síndrome geriátrico en evolución", *medicina.uc*, disponible en: https://medicina.uc.cl/publicacion/fragilidad-sindrome-geriatrico-evolucion/

- CASTRO-GIRONA MARTINEZ, A., "La reforma civil de la Ley 8/2021: el paradigma de los apoyos y el ejercicio de derechos en condiciones de igualdad", *hayderecho*, 29 de junio de 2021, disponible en: https://www.hayderecho.com/2021/06/29/la-reforma-civil-de-la-ley-8-2021-el-paradigma-de-los-apoyos-y-el-ejercicio-de-derechos-en-condiciones-de-igualdad/

- CEPD., "Las autoridades de protección de datos de la UE adoptan un dictamen conjunto sobre las propuestas de certificado digital verde", *edpb*, 6 de abril de 2021, disponible en: https://edpb.europa.eu/news/news/2021/eu-data-protection-authorities-adopt-joint-opinion-digital-green-certificate_es

- CERMI., "El impacto de la reforma del derecho civil", *riberdis*, 2021, disponible en: http://riberdis.cedid.es/handle/11181/6457

- CERMI., "La RAE enmienda el término "discpacidad" en el diccionario", *Cermi*, 24 de noviembre de 2020, disponible en: https://www.cermi.es/es/actualidad/noticias/la-rae-enmienda-el-t%C3%A9rmino-%E2%80%98discapacidad%E2%80%99-en-el-diccionario

- CÍNICA UNIVERSIDAD DE NAVARRA., "Diccionario médico", *cun*, disponible en: https://www.cun.es/diccionario-medico

- CIOMS y OMS., "Pautas éticas internacionales para la investigación relacionada con la salud con seres humanos", *cioms*, 2017, disponible en: https://cioms.ch/wp-content/uploads/2017/12/CIOMS-EthicalGuideline_SP_INTERIOR-FINAL.pdf

- COMISIÓN EUROPEA., "European data governance", *digital-strategy.ec.europa.eu*, 23 de junio de 2021, disponible en: https://digital-strategy.ec.europa.eu/en/policies/data-governance

- COMISIÓN EUROPEA. "¿Las personas pueden que sus datos se transfieran a otra organización?", *ec.europa.eu*, disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/dealing-citizens/can-individuals-ask-have-their-data-transferred-another-organisation_es

- COMISIÓN EUROPEA. "Preguntas y respuestas: Certificado COVID digital de la UE", *ec.europa.eu*, 1 de junio de 2021, disponible en: https://ec.europa.eu/commission/presscorner/detail/es/QANDA_21_2781

- COMISIÓN EUROPEA., "¿Podemos utilizar los datos para otro fin?", *ec.europa.eu*, disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/purpose-data-processing/can-we-use-data-another-purpose_es

- COMISIÓN EUROPEA., "¿Qué son los datos personales?", *ec.europa.eu*, disponible en: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es

- COMISIÓN EUROPEA., "Question and Answers on the interplay between the Clinical Trials Regulation and the General Data Protection Regulation", *health.ec.europa.eu*, disponible en: https://health.ec.europa.eu/system/files/2019-04/qa_clinicaltrials_gdpr_en_0.pdf

- CORCOBADO, M.A., "Estos son los permisos que concedes cuando instalas una app", *elpaís*, 31 de marzo de 2017, disponible en: https://elpais.com/tecnologia/2017/03/27/actualidad/1490626770_125439.html

- DANON, S., "GDPR Top Ten #6: Privacy by Design and by Default", *deloitte*, disponible en: https://www2.deloitte.com/ch/en/pages/risk/articles/gdpr-privacy-by-design-and-by-default.html

- DAVIS, R., "What do Health Research Regulations 2018 mean for health researchers?", *hrb*, 19 de octubre de 2018, p. 4, disponible en: https://www.hrb.ie/fileadmin/1._Non-plugin_related_files/RSF_files/GDPR_guidance_for_researchers/What_do_Health_Research_Regulations_2018_mean_for_health_researchers_-_Ruth_Davies.pdf

- DCU., "Data Protection Impact Assessment", *dcu*, disponible en: https://www.dcu.ie/search-

results?cx=017566043542663844620%3Ag9uk5n1hgmy&cof=FORID%3A11&keywords=Project+Screening+Questionnaire+Introduction&x=0&y=0

- DE LORENZO APARICI, O., "Problemática de las anotaciones subjetivas de la Ley 41/2002", *aeds*, 2006, disponible en: https://www.aeds.org/congreso/congresos-aeds/ponencias/Ofelia%20de%20Lorenzo.pdf

- DE VERDA Y BEAMONTE, J.R., "¿Es posible seguir distinguiendo entre capacidad jurídica y capacidad de obrar?", *idibe*, 30 de septiembre de 2021, disponible en: https://idibe.org/tribuna/posible-seguir-distinguiendo-capacidad-juridica-capacidad-obrar/

- DEPARTAMENTO DE SALUD DEL GOBIERNO VASCO., "Transparencia sobre el nuevo coronavirus (COVID-19)", *euskadi.eus*, 26 de mayo de 2021, disponible en: https://www.euskadi.eus/vacunacion/web01-a3txerto/es/

- DEPARTMENT OF HEALTH; HEALTH SERVICES EXECUTIVE; HRB Y SECRETARIAT TO HEALTH RESEARCH CONSENT DECLARATION COMMITTE., "Guidance on informed Consent obtained in the time of EU Directive Amendment to the Health Research Regulations", 2021, *hseresearch*, disponible en: https://hseresearch.ie/data-protection-and-research/

- DPC., "The Data Protection Commission", *dataprotection*, disponible en: https://www.dataprotection.ie/

- ECONOMIST & JURIST., "5 preguntas sobre la nueva guía de protección de datos por defecto", *economistjurist*, 11 de noviembre de 2020, disponible en: https://www.economistjurist.es/noticias-juridicas/5-preguntas-sobre-la-nueva-guia-de-proteccion-de-datos-por-defecto/

- EDPS., "Privacy by default", *edps*, disponible en: https://edps.europa.eu/data-protection/our-work/subjects/privacy-default_en

- EISS, R., "Confusion over data-privacy law stalls scientific progress", *nature*, 25 de agosto de 2020, disponible en: https://www.nature.com/articles/d41586-020-02454-7

- ELGA., "About", *elga.gv.at*, disponible en: https://www.elga.gv.at/en/about-elga/

- ELGA., "Schulungsunterlagen: Textbausteine zur Ergänzung und Unterstützung eigener Schulungsunterlagen", *elga.gv.at*, 16 de febrero de 2016, disponible en: https://www.elga.gv.at/fileadmin/user_upload/Dokumente_PDF_MP4/Technisches/ELGA_Basis_fuer_Schulungsunterlagen_V2.0.pdf

- EQUIPO GIMÉNEZ SALINAS., "Principales novedades de la Ley 8/2021 por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad y Derecho Ley 19/2021 en Cataluña", *gimenez-salinas.es,* 26 de octubre de 2021, disponible en: https://gimenez-salinas.es/novedades-ley-8-2021-apoyo-personas-discapacidad/

- EUROPEAN PRIVACY SEAL., "EuroPriSe - Sello Europeo de Privacidad", *europrivacyseal,* disponible en: https://www.euprivacyseal.com/EPS-en/Europrise-sello-europeo-de-privacidad

- FDA., "Cybersecurity Vulnerabilities Identified in St. Juse Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication", *wayback,* 9 de enero de 2017, disponible en: https://wayback.archive-it.org/7993/20201222110135/https://www.fda.gov/medical-devices/safety-communications/cybersecurity-vulnerabilities-identified-st-jude-medicals-implantable-cardiac-devices-and-merlinhome

- FLEISCHER, P., "The right to be forgotten, or how ti edut your history", *pteterfleischer.blogspot*, 29 de enero de 2012, disponible en: http://peterfleischer.blogspot.com/2011/03/foggy-thinking-about-right-to-oblivion.html

- FUNDACIÓN ALZHEIMER ESPAÑA., "Teleasistencia: ¿Qué es? ¿En qué consiste? ¿Cómo contratarlo?", *alzfae,* disponible en: http://www.alzfae.org/fundacion/459/teleasistencia-que-es-en-que-consiste-como-contratarlo

- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI., "Faq", *garanteprivacy,* 2021, disponible en: https://www.garanteprivacy.it/temi/coronavirus/faq

- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI., "Fascicolo sanitario elettronico-Domande più frequenti", *garanteprivacy*, disponible en: https://www.garanteprivacy.it/faq/fascicolo-sanitario

- GARANTE PER LA PROTEZIONE DEI DATI PERSONALI., "Fascicolo sanitario elettronico (FSE)", *garanteprivacy*, 11 de enero de 2021, disponible en: https://www.garanteprivacy.it/temi/fse

- GARCÍA MARTÍNEZ, N. y BERMEJO NIETO, A., "Tecnologías de la información y las comunicaciones para las personas mayores", *upm*, 2004, disponible en: https://www.upm.es/sfs/Rectorado/Organos%20de%20Gobierno/Consejo%20Social/Actividades/tecnologias_informacion_comunicaciones.pdf

- GENERALITAT VALENCIANA., "Telemonitorización en pacientes con patologías crónicas en Atención Primaria. Programa Valcrònic", *publicaciones.san.gva*, 2016, disponible en: http://publicaciones.san.gva.es/publicaciones/documentos/V.1481-2016.pdf

- GESTADATA CONSULTING., "El consentimiento según el RGPD", *gestadataconsulting*, 31 de julio de 2020, disponible en: https://www.gesdataconsulting.es/consentimiento-segun-el-rgpd/

- GOMÁ LANZÓN, F., "Los poderes preventivos en la ley de apoyo a las personas con discapacidad", *hayderecho*, 8 de junio de 2021, disponible en: https://www.hayderecho.com/2021/06/08/los-poderes-preventivos-en-la-ley-de-apoyo-a-las-personas-con-discapacidad/

- GÓMEZ PIQUERAS, C., "Contenido, usos y finalidad de la historia clínica", *ponencia en la AEPD*, 25 de febrero de 2008, disponible en: https://www.redipd.org/sites/default/files/2020-01/ponencia3_250208.pdf

- GONZÁLEZ, Y., "La información por capas en el RGPD", *grupoatico34*, 27 de marzo de 2020, disponible en: https://protecciondatos-lopd.com/empresas/informacion-por-capas-rgpd/

- GORETTA, R., "Autorizzazioni generali dopo il GDPR, cosa cambia", *agendadigitale*, 28 de enero de 2019, disponible en: https://www.agendadigitale.eu/sicurezza/autorizzazioni-generali-dopo-il-gdpr-cosa-cambia/

- GRUPO DE TRABAJO SOBRE DERECHOS DIGITALES DE LOS CIUDADANOS., "Primer conversatorio de derechos digitales de los ciudadanos", *red*, 31 de mayo de 2017, disponible en: https://www.red.es/redes/es/magazin-red/reportajes/el-primer-conversatorio-sobre-los-derechos-digitales-sit%C3%BAa-espa%C3%B1a-la

- HARARI, Y.N., "The world after coronavirus", *financialtimes*, 20 de marzo de 2020, Disponible en: https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

- HRB., "Assessment of applications for consent declarations", *hrb*, disponible en: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/consent/health-research-consent-declaration-committee/

- HRB., "Broad consent and the Health Research Regulations 2018", *hrb*, disponible en: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/gdpr-and-health-research/consent/broad-consent/

- HRB., "Frequently asked questions", *hrb*, disponible en: https://www.hrb.ie/funding/manage-a-grant/faq/

- HRB., "Health Research Regulations 2018 FAQ", *hrb*, disponible en: https://www.hrb.ie/funding/gdpr-guidance-for-researchers/health-research-regulations-2018/health-research-regulations-2018-faq/

- HRB., "New National Research Ethics Committe for Covid-19 research", *hrb*, 20 de abril de 2020, disponible en: https://www.hrb.ie/news/covid-19-coronavirus/coronavirus-news/article/new-national-ethics-committee-for-covid-19-research/

- HRCDC,. "Decision tree: Can I apply for a consent declaration?", *hrcdc*, disponible en: https://hrcdc.ie/wp-content/uploads/2019/01/Decision_Tree_30072018.pdf

- HRCDC., "About us", *hrcdc*, disponible en: https://hrcdc.ie/about-us/

- HRCDC., "guidance", *hrcdc*, disponible en: https://hrcdc.ie/guidance/

- HRCDC., "Meeting", *hrcdc*, 15 de abril de 2020, disponible en: https://hrcdc.ie/wp-content/uploads/2020/05/HRCDC-Meeting-Minutes-15.04.2020-APPROVED.pdf

- HRCDC., "Overview", *hrcdc*, disponible en: https://hrcdc.ie/about-us/#Overview

- HSE., "Data Protection Impact Assessment Covid Tracker App", *hse*, 26 de junio de 2020, disponible en: https://www.hse.ie/eng/services/news/newsfeatures/covid19-updates/covid-tracker-app/covid-tracker-app.html

- HSE., "Data Requests", *hse*, disponible en: https://www.hse.ie/eng/gdpr/data-requests/

- HSE., "General Data Protection Regulation (GDPR) Frequently asked questions (Faqs)", *hse*, disponible en: https://www.hse.ie/eng/gdpr/gdpr-faq/hse-gdpr-faqs-public.pdf

- HURKOA., Informe del proyecto de fragilidad, *hurkoa*, 2018, p. 18, disponible en: https://www.hurkoa.eus/sites/default/files/memorias/INFORME_FRAGILIDAD2018_ES_WEB.pdf

- IMMUNI., "Cos'è Immuni?", *immuni.italia*, disponible en: https://www.immuni.italia.it/faq.html

- IBERLEY., "Condiciones del consentimiento en materia de protección de datos en el Reglamento General de Protección de Datos (RGPD) y en la LO 3/2018

(LOPDGDD)", *iberley*, 30 de enero de 2019, disponible en: https://www.iberley.es/temas/condiciones-aplicables-consentimiento-materia-proteccion-datos-62815

- IBERLEY., "Consentimiento explícito en el Reglamento General de Protección de Datos (RGPD) y en la LO 3/2018 (LOPDGDD)", *iberley*, 30 de enero de 2019, disponible en: https://www.iberley.es/temas/consentimiento-explicito-materia-proteccion-datos-62819#:~:text=El%20t%C3%A9rmino%20expl%C3%ADcito%20se%20refiere,una%20declaraci%C3%B3n%20expresa%20de%20consentimiento

- IBERLEY., "Derecho de transparencia e información en la LO 3/2018 (LOPDGDD) y en el Reglamento General de Protección de Datos (RGPD)", *iberley*, 18 de enero de 2019, disponible en: https://www.iberley.es/temas/derecho-transparencia-informacion-lopdgdd-rgpd-62754

- ICO., "Are there any exceptions or exemptions?", *ico*, disponible en: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/are-there-any-exceptions/

- ICS., "What is privacy by design & default?", *ics*, disponible en: https://www.ics.ie/news/what-is-privacy-by-design-a-default

- ILUSTRE COLEGIO DE ABOGADOS DE MADRID., "Ley 8/2021, de 2 de junio, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica: cuadro comparativo", *web.icam*, 7 de junio de 2021, disponible en: https://web.icam.es/informacion-de-interes-profesional-cuadros-comparativos-con-las-modificaciones-introducidas-por-la-ley-8-2021-de-2-de-junio-y-por-la-ley-organica-8-2021-de-4-de-junio/

- INE., "Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares Año 2020", *ine*, 16 de noviembre de 2020, disponible en: https://www.ine.es/prensa/tich_2020.pdf

- INSTITUTO DE INFORMACIÓN SANITARIA., "El sistema de historia clínica digital", *mscbs*, disponible en: https://www.mscbs.gob.es/organizacion/sns/planCalidadSNS/docs/HCDSNS_Castellano.pdf

- IRISH MEDICAL TIMES., "Data protection impact on health research assessed", *imt*, 11 de enero de 2019, disponible en: https://www.imt.ie/clinical/data-protection-impact-health-research-assessed-17-01-2019/

- ISO., "Organismos Nacionales de Normalización en Países en Desarrollo", *iso*, p. 1, disponible en: https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/fast_forward-es.pdf

- JOYANES AGUILAR, L.; POYATOS DÍAZ, J.M., "Big Data y el sector de la salud: el futuro de la sanidad". *Blog Juan Miguel Poyatos*, 2013, disponible en: http://poyatosdiaz.com/index.php/big-data-y-el-sector-de-la-salud-el-futuro-de-la-sanidad

- JUNTA DE ANDALUCIA., "Distintivo AppSaludable", *calidadappsalud*, disponible en: http://www.calidadappsalud.com/distintivo-appsaludable/

- LA MONCLOA., "Reforma del artículo 49 de la Constitución española", *lamoncloa*, 11 de mayo de 2021, disponible en: https://www.lamoncloa.gob.es/consejodeministros/Paginas/enlaces/110521-enlace-constitucion.aspx

- LARRUCEA RODRIGO, C., "Mhealth y Bigdata en sanidad", *Blog Derecho y salud no van siempre de la mano*, 14 de abril de 2016, disponible en: https://carmenrodrigodelarrucea.wordpress.com/2016/04/14/mhealth-y-bigdata-en-sanidad/

- LENNON, P., "Examining the concept of consent from a legal perspective in health research", *tcd*, 28 de abril de 2021, disponible en: https://www.tcd.ie/dataprotection/healthresearch/

- LINDE, P., "La Fiscalía del Supremo censura la vacunación forzosa", *elpaís*, 25 de febrero de 2021, disponible en: https://elpais.com/sociedad/2021-02-25/la-fiscalia-del-supremo-censura-la-vacunacion-forzosa.html

- MARINI, P., "Dati sensibili e GDPR: il provvedimento del Garante", *Altalex*, 31 de julio de 2019, disponible en: https://www.altalex.com/documents/news/2019/07/31/dati-sensibili-gdpr-garante

- MARTÍN-LESENDE, I.; ORRUÑO, E.; BAYÓN, J.C.; BILBAO, A.; VERGARA, I.; CAIRO, M.C.; ASUA, J.; ROMO, M.I.; ABAD, R., REVIRIEGO, E. Y LARRAÑAGA, J., "Evaluación e impacto de una intervención de telemonitorización en pacientes domiciliarios con insuficiencia cardiaca o broncopatía crónica controlada desde la atención primaria. Ensayo clínico aleatorizado. Estudio TELBIL". *Servicio Central de Publicaciones del Gobierno Vasco*, 2013, disponible en: https://www.osakidetza.euskadi.eus/contenidos/informacion/2013_osteba_publicacion/es_def/adjuntos/INTERVENCION%20DE%20TELEMONITORIZACION.pdf

- MARZO PORTERA, A., "El interés público de los datos personales en tiempos del COVID-19", *hayderecho*, 10 de abril de 2020, disponible en: https://hayderecho.expansion.com/2020/04/10/el-interes-publico-de-los-datos-personales-en-tiempos-del-covid-19/

- MELL, P. y GRANCE, T., The NIST definition of Cloud computing: Recommendations of the National institute of Standards and Technology, *National institute of Standards and Technology*, 2011, p.2, disponible en: http://faculty.winthrop.edu/domanm/csci411/Handouts/NIST.pdf

- MINISTERIO DE SANIDAD., "Inventario de actividades de tratamiento de datos personales de las unidades que estaban integradas en el extinto ministerio de sanidad, consumo y bienestar social", *mscbs*, 23 de agosto de 2022, disponible en: https://www.mscbs.gob.es/servCiudadanos/proteccionDatos/docs/RAT_MSCBS.pdf

- MINISTERIO DE SALUD., "Estrategia de salud digital", *sanidad.gob.es*, 2 de diciembre de 2021, disponible en: https://www.sanidad.gob.es/ciudadanos/pdf/Estrategia_de_Salud_Digital_del_SNS.pdf

- MUIÀ P.P., "Le prescrizioni del Garante privacy relative al trattamento di dati personali effettuato per scopi di ricerca scientifica", *diritto.it*, 12 de septiembre de 2019, disponible en: https://www.diritto.it/le-prescrizioni-del-garante-privacy-relative-al-trattamento-di-dati-personali-effettuato-per-scopi-di-ricerca-scientifica/

- NCHD., "What does that mean?", *Irishmedicaltimes*, 10 de mayo de 2017, disponible en: https://www.imt.ie/opinion/letters/nchd-what-does-that-mean-10-05-2017/

- NETFLIX. "The social dilemma", *netflix*, disponible en: https://www.netflix.com/es/title/81254224

- NHS., "Scottish Patients at Risk of Readmission and Admission (SPARRA). Developing Risk Prediction to Support Preventative and Anticipatory Care in Scotland", Health and Social Care Information Programme, 2011, disponible en: https://www.isdscotland.org/Health-Topics/Health-and-Social-Community-Care/SPARRA/2012-02-09-SPARRA-Version-3.pdf

- NREC COVID-19., "Apply", *hrb*, disponible en: https://www.hrb.ie/covid-19-ethical-review/apply/

- NREC COVID-19., "Decisions", *nrecoffice*, disponible en: https://www.nrecoffice.ie/committees/nrec-covid-19/decisions/

- NREC COVID-19., "Overview", *hrb*, disponible en: https://www.hrb.ie/covid-19-ethical-review/nrec-covid-19-overview/

- O´CONNOR, M., "Health Research Regulations 2018: Context and purpose", *hrb*, 19 de octubre de 2018, p.5, disponible en: https://www.hrb.ie/fileadmin/1._Non-plugin_related_files/RSF_files/GDPR_guidance_for_researchers/Health_Research_Regulations_2018_-_Context_and_purpose_-_Muiris_O__Connor.pdf

- OBSERVATORIO DE BIOÉTICA Y DERECHO DE LA UNIVERSIDAD DE BARCELONA., "Presentada la metodología de evaluación de impacto relativa a la protección de datos en salud", *bioeticayderecho*, 9 de febrero de 2021, disponible en: http://www.bioeticayderecho.ub.edu/es/presentada-la-metodologia-de-evaluacion-del-impacto-relativa-la-proteccion-de-datos-en-salud

- OMS., "Clasificación Internacional del funcionamiento, de la discapacidad y de la salud", *imserso*, 2001, p. 14, disponible en: https://www.imserso.es/InterPresent2/groups/imserso/documents/binario/435cif.pdf

- OMS., "mHealth: New horizons for health through mobile technologies", *app.who*, 2011, p. 6, disponible en: http://apps.who.int/iris/bitstream/handle/10665/44607/9789241564250_eng.pdf?sequence=1

- OMS., "The protection of personal data in health information systems- principles and processes for publich health", *apps.who*, 2021, disponible en: https://apps.who.int/iris/handle/10665/341374?locale-attribute=fr&

- OPS y OMS., "Marco de implementación de un servicio de telemedicina", 2016, disponible en: https://iris.paho.org/bitstream/handle/10665.2/28413/9789275319031_spa.pdf?sequence=6&isAllowed=y

- OSAKIDETZA., "Carpeta de salud", *osakidetza.euskadi.eus*, disponible en: https://www.osakidetza.euskadi.eus/servicios-on-line/-/carpeta-de-salud/

- OSTEC., "¿Qué significa "privacy by design" y cuál es su relación con la ley de protección de datos?", *ostec.blog*, 29 de julio de 2019, disponible en: https://ostec.blog/es/generico/privacy-by-design/

- PINDADO GALÁN, M. y MARRERO MACÍAS, R., "Desarrollos normativos derivados de la Convención sobre los derechos de las personas con discapacidad en España. Una perspectiva desde los derechos de las personas con trastorno del espectro del autismo", *riberdis*, 2022, disponible en: http://riberdis.cedd.net/handle/11181/6509

- PUYOL, J. "El régimen legal de las apps", *confilegal*, 2 de marzo de 2016, disponible en: https://confilegal.com/20150420-el-regimen-legal-de-las-apps/

- RAE., Definición de ancianidad, disponible en: https://dle.rae.es/ancianidad

- RAE., Definición de discapacidad, disponible en: https://dle.rae.es/discapacidad

- RAE., Definición de frágil, disponible en: https://dle.rae.es/fr%C3%A1gil

- RAE., Definición de fragilidad, disponible en: https://dle.rae.es/fragilidad

- RAE., Definición de la inteligencia artificial, disponible en: https://dle.rae.es/inteligencia

- RAE., Definición de tácito, disponible en: https://dle.rae.es/t%C3%A1cito

- RECIO GAYO, M., "Protección de datos desde el diseño: principio y obligación en el RGPD", *elderecho*, 20 de febrero de 2017, disponible en: https://elderecho.com/proteccion-de-datos-desde-el-diseno-principio-y-obligacion-en-el-rgpd

- RIZZO, M.L., "Ricerca scientifica e Covid-19: Le basi giuridiche per trattare i dati dei pazienti per un utilizzo secondario", *Riskmanagemente360*, 2 de septiembre de 2020, disponible en: https://www.riskmanagement360.it/compliance/ricerca-scientifica-e-covid-19-le-basi-giuridiche-per-trattare-i-dati-dei-pazienti-per-un-utilizzo-secondario/

- ROCA TRÍAS, E., "Voto particular discrepante que formula la Magistrada doña Encarnación Roca Trías a la Sentencia dictada en el recurso de inconstitucionalidad núm. 4751-2017", *tribunalconstitucional*, 17 de enero de 2019, disponible en: https://www.tribunalconstitucional.es/NotasDePrensaDocumentos/NP_2019_002/2017-4751VPS.pdf

- RODRÍGUEZ PITA, P., "Reglamento sobre gobernanza de los datos", *economiadigital*, 5 de diciembre de 2020, disponible en: http://economiadigital.etsit.upm.es/reglamento-sobre-la-gobernanza-de-los-datos/

- ROSEN, J., "The web means the end of forgetting", *nytimes*, 21 de Julio de 2010, disponible en: http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html

- RUBIO, I., "Por qué puede ser peligroso que un algoritmo decida si contratarte o concederte un crédito", *elpais*, 23 de noviembre de 2018, disponible en: https://elpais.com/tecnologia/2018/11/19/actualidad/1542630835_054987.html

- RUTE, H., "¿Qué es la fragilidad en los adultos mayores?", *ipsuss*, 16 de mayo de 2018, disponible en:http://www.ipsuss.cl/ipsuss/columnas-de-opinion/que-es-la-fragilidad-en-los-adultos-mayores/2018-05-16/165708.html

- SALVADOR CODERCH, P., "Entre recordar y olvidar", *elpais* 1 de junio de 2011, disponible en: https://elpais.com/diario/2011/06/01/opinion/1306879205_850215.html

- SÁNCHEZ, J.L., "La liga de futbol usa el micrófono del teléfono de millones de aficionados para espiar a los bares", *eldiario*, 10 de junio de 2018, disponible en: https://www.eldiario.es/tecnologia/Liga-Futbol-microfono-telefono-aficionados_0_780772124.html

- SHMERLING MAGAZANIK, L., "Using Health Data for Research: Evolving National Policies", *techpolicy*, 2021, disponible en: https://techpolicy.org.il/wp-content/uploads/2021/02/Using-Health-Data-for-Research-Evolving-National-Policies-FV-.pdf

- SOCIEDAD ESPAÑOLA DE SALUD PÚBLICA y ADMINISTRACIÓN SANITARIA., "Protección de datos personales y secreto profesional en el ámbito de la salud: una propuesta normativa de adaptación al RGPD", *sespas*, 2017, disponible en: https://sespas.es/wp-content/uploads/2018/02/SESPAS_informe_proteccion_datos_2017.pdf

- THE EUROPEAN COMMISSION'S HIGH-LEVEL EXPERT GROUP ON ARTIFICIAL INTELLIGENCE., "A definitión of AI: Main capabilities and Disciplines", *ec.europa.eu*, 2019, disponible en: https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf

- THE GUARDIAN., "Releaved: how drugs giants can access your health records", *theguardian*, 8 de febrero de 2020, disponible en: https://www.theguardian.com/technology/2020/feb/08/fears-over-sale-anonymous-nhs-patient-data#:~:text=The%20Department%20of%20Health%20and,leading%20experts%20in%20the%20field

- TRINITY COLLEGE DUBLIN., "Guidance on the Assessment of explicit consent for health research", *tcd*, 2019, disponible en: https://nursing-midwifery.tcd.ie/research/assets/pdf/consent-form.pdf

- UNATE., "Eliminemos las acepciones despectivas en la definición de vejez", *change.org*, disponible en: https://www.change.org/p/real-academia-espa%C3%B1ola-cambio-en-la-definici%C3%B3n-de-la-palabra-vejez-en-la-rae

- UODO., "The first fine imposed by the President of the Personal Data Office", *uodo*, 3 de junio de 2019, disponible en: https://uodo.gov.pl/en/553/1009

- VELILLA ANTOLÍN, N., "Una visión crítica a la Ley de apoyo a las personas con discapacidad", *elnotario*, 2022, disponible en: https://www.elnotario.es/opinion/opinion/10938-una-vision-critica-a-la-ley-de-apoyo-a-las-personas-con-discapacidad

- VEREKER, E., "HRCDC", *tcd*, 28 de abril de 2021, disponible en: https://www.tcd.ie/tcaid/research/healthresearchregulations.php

- VIVAS TESÓN, I., "La reforma civil y procesal para el apoyo de las personas con discapacidad: ¿A partir de septiembre, qué?", *hayderecho*, 13 de junio de 2021, disponible en: https://www.hayderecho.com/2021/06/13/la-reforma-civil-y-procesal-para-el-apoyo-de-las-personas-con-discapacidad-a-partir-de-septiembre-que/

- WARMAN, M., "Vint Cerf attacks European internet policy", *telegraph*, 29 de marzo de 2012, disponible en: https://www.telegraph.co.uk/technology/news/9173449/Vint-Cerf-attacks-European-internet-policy.html

NORMATIVA:

- **Europea e internacional:**

- Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022 relativo a la gobernanza de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos)

- Directiva (UE) 2019/1024 del Parlamento Europeo y del Consejo, de 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público

- Reglamento 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre los productos sanitarios

- Reglamento (CE) 1338/2008, del Parlamento Europeo y del Consejo, de 16 de diciembre de 2008, sobre estadísticas comunitarias de salud pública y de salud y seguridad en el trabajo

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento

de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)

- Reglamento (UE) 536/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los ensayos clínicos de medicamentos de uso humano, y por el que se deroga la Directiva 2001/20/CE

- Reglamento (CE) 765/2008 del Parlamento Europeo y del Consejo de 9 de julio de 2008 por el que se establecen los requisitos de acreditación y vigilancia del mercado relativos a la comercialización de los productos y por el que se deroga el Reglamento (CEE) núm. 339/93

- Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos

- Convención sobre los derechos de las personas con discapacidad, hecho en Nueva York el 13 de diciembre de 2006

- Carta de los Derechos Fundamentales de la Unión Europea de 18 de diciembre de 2000 (2000/C 364/01)

- Decisión 1082/2013/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud
- ISO/IEC 17000:2004. Evaluación de la conformidad. Vocabulario y principios generales

- **<u>Nacional:</u>**

- Constitución Española de 29 de diciembre de 1978

- Ley 8/2021, de 2 de junio de 2021, por la que se reforma la legislación civil y procesal para el apoyo a las personas con discapacidad en el ejercicio de su capacidad jurídica

- Ley 15/2015, de 2 de julio de 2015 de la Jurisdicción Voluntaria

- Ley 33/2011, de 4 de octubre de 2011, General de Salud Pública

- Ley 20/2011, de 21 de julio de 2011, del Registro Civil

- Ley 18/2011, de 5 de julio de 2011, reguladora del uso de las tecnologías de la información y la comunicación en la Administración de Justicia

- Ley 26/2011, de 1 de agosto de 2011, de adaptación normativa a la Convención de Derechos de las Personas con Discapacidad

- Ley 1/2009, de 25 de marzo de 2009, de reforma de la Ley de 8 de junio de 1957 sobre el Registro Civil, en materia de incapacitaciones, cargos tutelares y administradores de patrimonios protegidos

- Ley 14/2007, de 3 de julio de 2007, de Investigación biomédica

- Ley 49/2007, de 26 de diciembre de 2007, por la que se establece el régimen de infracciones y sanciones en materia de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad

- Ley 14/2006, de 26 de mayo de 2006, sobre Técnica de Reproducción Humana Asistida

- Ley 51/2003, de 2 de diciembre de 2003, de igualdad de oportunidades, no discriminación y accesibilidad universal de las personas con discapacidad

- Ley 7/2002, de 12 de diciembre de 2002, de las voluntades anticipadas en el ámbito de la sanidad

- Ley 41/2002, de 14 de noviembre de 2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

- Ley 34/2002, de 11 de julio 2002, de servicios de la sociedad de la información y de comercio electrónico

- Ley 14/1986, de 25 de abril de 1986, General de Sanidad

- Ley 13/1982, de 7 de abril 1982, de integración social de los minusválido

- Ley de Notariado de 28 de mayo de 1862

- Ley Orgánica 11/2021, de 28 de diciembre de 2018, de lucha contra el dopaje en el deporte en el deporte

- Ley Orgánica 3/2018, de 5 de diciembre de 2018, de Protección de Datos Personales y garantía de los derechos digitales

- Ley Orgánica 15/1999, de 13 de diciembre 1999, de Protección de Datos de Carácter Personal (derogada)

- Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19

- Real Decreto-ley 9/2014, de 4 de julio de 2014, por el que se establecen las normas de calidad y seguridad para la donación, la obtención, la evaluación, el procesamiento, la preservación, el almacenamiento y la distribución de células y tejidos humanos y se aprueban las normas de coordinación y funcionamiento para su uso en humano

- Real Decreto 1720/2007, de 21 de diciembre de 2007, por el que se aprobaba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal

- Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil

- Orden SND/404/2020, de 11 de mayo, de medidas de vigilancia epidemiológica de la infección por SARS-CoV-2

- Orden SSI/81/2017, de 19 de enero, por la que se publica el Acuerdo de la Comisión de Recursos Humanos del Sistema Nacional de Salud, por el que se aprueba el protocolo mediante el que se determinan pautas básicas destinadas a asegurar y proteger el derecho a la intimidad del paciente por los alumnos y residentes en Ciencias de la Salud.

- **<u>Autonómica:</u>**

- Ley 10/2017, de 27 de junio, de las voluntades digitales y de modificación de los libros segundo y cuarto del Código Civil de Cataluña

- Ley Foral 17/2010 de 8 de noviembre de derechos y deberes de las personas en materia de salud en la comunidad foral de Navarra

- Ley 3/2005, de 8 de julio de información sanitaria y autonomía del paciente de Extremadura

- Ley 9/1998, de 15 de julio, del Código de Familia de Cataluña

- Decreto 38/2012, de 13 de marzo, sobre historia clínica y derechos y obligaciones de pacientes y profesionales de la salud en materia de documentación clínica del País Vasco

- Decreto 144/2011, de 28 de junio, del servicio público de teleasistencia[1025] del País Vasco

- Decreto 24/2011, de 12 de abril de la documentación sanitaria de la Castilla la Mancha

- Decreto 29/2009, de 5 febrero, por el que se regula el uso y acceso a la historia clínica electrónica

- Decreto 45/1998 de 17 de marzo, por el que se establece el contenido y se regula la valoración, conservación y expurgo de los documentos del Registro de Actividades Clínicas de los Servicios de Urgencias de los Hospitales y de las Historias Clínicas Hospitalarias.

- Decreto 272/1986 de 25 de noviembre de 1986 por el que se regula el uso de la Historia Clínica de los centros Hospitalarios de la Comunidad Autónoma del País Vasco

- **<u>Extranjera:</u>**

  - **Italia:**

- Decreto Legislativo 101/2018 10 agosto 2018, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonche' alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)

- Decreto Legislativo 196/2003 30 giugno 2003, Codice in materia di protezione dei dati personali

- Decreto legge 179/2012, 18 ottobre 2012, Ulteriori misure urgenti per la crescita del Paese

- Autorizzazione n. 1/2016, Autorizzazione al trattamento dei dati sensibili nei rapporti di lavoro, 15 dicembre 2016

- Autorizzazione n. 3/2016, Autorizzazione al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni, 15 dicembre 2016

[1025] BOPV núm. 124 de 30 de Junio de 2011

- Autorizzazione n. 6/2016, Autorizzazione al trattamento dei dati sensibili da parte degli investigatori privati, 15 diciembre 2016

- Autorizzazione n. 8/2016, Autorizzazione generale al trattamento dei dati genetici, 15 dicembre 2016

- Autorizzazione n. 9/2016, Autorizzazione generale al trattamento de dati personali effettuato per scopi di ricerca scientifica, 15 dicembre 2016

- Provvedimento recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1 del d.lgs. 10 agosto 2018, n. 101

▪ **Irlanda:**

- 7/2018 Data Protection Act 2018, 24th May 2018

- S.I. No. 18/2021 Data Protection Act 2018 (Section 36(2)) (Health Research) Regulations 2018

- 15/2014 Health identifiers act 2014, 8th July 2014

- 6/2003 Data Protection (Amendment) Act 2003, 10th April 2003

- 25/1988 Data Protection Act 1988, 13th July 1988

▪ **Austria:**

- ELGA-Verordnung 2015, 12 mai 2015, BGBl. II Nr. 106/2015

- Gesundheitstelematikgesetzes 2012 (GTelG 2012), 14 dezember 2012, BGBl. I Nr. 111/2012

▪ **Francia:**

- LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique

<u>JURISPRUDENCIA:</u>

- STJUE (Sala Cuarta), de 27 de octubre de 2022, Proximus NV contra Gegevensbeschermingsautoriteit, C-129/21, ECLI:EU:C:2022:833

- STJUE (Sala Primera), de 20 de octubre de 2022, Digi Távközlési és Szolgáltató Kft contra Nemzeti Adatvédelmi és Információszabadság Hatóság, C-77/21, ECLI:EU:C:2022:805

- STJUE (Sala Quinta), de 24 de febrero de 2022, SS SIA contra Valsts ieņēmumu dienests, C-175/20, ECLI:EU:C:2022:124

- STJUE (Sala Segunda), de 11 de noviembre de 2020, Orange Romania, C-61/19, ECLI:EU:C:2020:901

- STJUE (Gran Sala), de 1 de octubre de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801

- STJUE, de 24 de septiembre de 2019, Google contra CNIL, C-507/17, ECLI:EU:C:2019:772

- STJUE (Gran Sala), de 24 de septiembre de 2019, C-136/17, ECLI:EU:C:2019:773

- STJUE (Sala Segunda), de 29 de julio de 2019, Fashion ID, C-40/17, ECLI:EU:C:2019:629

- TJUE (Gran Sala), Conclusiones del abogado general, de 21 de marzo de 2019, Planet 49, C-673/17, ECLI:EU:C:2019:801

- STJUE (Gran Sala), de 10 de julio de 2018, Jehovan todistajat, C–25/17, ECLI:EU:C:2018:551

- STJUE (Sala Segunda), de 20 de diciembre 2017, Peter Nowak contra Data Protection Commissioner, asunto C-434/16, ECLI:EU:C:2017:994

- TJUE (Gran Sala) Dictamen 1/15 de 26 julio 2017, ECLI:EU:C:2017:592

- STJUE (Gran Sala) de 13 de mayo de 2014, Google Spain, S.L. y Google Inc. contra la AEPD y Mario Costeja González, asunto C-131/12, ECLI:EU:C:2014:317

- STJUE (Sala primera) de 10 de diciembre de 2010, (Land Nordrhein-Westfalen contra D.-H. T.), asunto C-620/19, ECLI:EU:C:2020:1011

- STJUE (Sala tercera) de 7 de mayo de 2009, (College van burgemeester en wethouders van Rotterdam contra M. E. E. Rijkeboer) asunto C-553/07, ECLI:EU:C:2009:293

- STEDH 33117/02, 22 de enero de 2013, asunto Lashin contra Rusia

- STEDH 38832/06 de 20 de mayo de 2010, asunto Alajos Kiss contra Hungría

- STEDH 44009/05, de 27 de marzo de 2008, asunto Chtoukatourov contra Rusia

- STEDH 14461/88, de 9 de julio de 1991, asunto Yvonne Chave née Jullien contra Francia

- Sentencia del Tribunal de la Haya C/09/550982 / HA ZA 18-388 de 5 de febrero de 2020, (ECLI: NL: RBDHA: 2020: 865)

- Resolución de la Asamblea General de Naciones Unidas 56/168, de 19 de diciembre de 2001

- Resolución de la Asamblea General de las Naciones Unidas 217 A (III) de 10 de diciembre de 1948

- STS Sala de lo Civil 734/2021, de 2 de noviembre de 2021 (Rec. Núm. 1201/2021)

- STS Sala de lo Civil 706/2021, de 19 de octubre de 2021 (Rec. Núm. 305/2021)

- STS Sala de lo Civil 269/2021, de 6 de mayo de 2021 (Rec. Núm. 2235/2020)

- STS Sala de lo Penal 326/2019, de 20 de junio de 2020 (Rec. Núm. 998/2018)

- STS Sala de lo Civil 118/2020, de 19 de febrero de 2020 (Rec. Núm. 3904/2019)

- STS Sala de lo Civil 465/2019, de 17 de septiembre de 2019 (Rec. Núm. 5199/2018)

- STS Sala de lo Contencioso-administrativo, sección 3ª, 1062/2019 de 12 de julio de 2019 (Rec. Núm. 4980/2018)

- STS Sala de lo Civil 458/2018, de 18 de julio de 2018 (Rec. Núm. 4374/2017)

- STS Sala de lo Civil 362/2018, de 15 de mayo 2018 (Rec. Núm. 2122/2017)

- STS Sala de lo Civil 124/2018, de 7 de marzo de 2018 (Rec. Núm. 4192/2016)

- STS Sala de lo Civil 118/2018, de 6 de marzo de 2018 (Rec. Núm. 1632/2017)

- STS Sala de lo Civil 552/2017, de 11 de octubre de 2017 (Rec. Núm. 2065/2016)

- STS Sala de lo Civil 530/2017, de 27 de septiembre de 2017 (Rec. Núm. 183/2017)

- STS Sala de lo Civil 298/2017, de 16 de mayo de 2017 (Rec. Núm. 298/2017)

- STS Sala de lo Civil 216/2017, de 4 de abril de 2017 (Rec. Núm. 56/2016)

- STS Sala de lo Civil 373/2016, de 3 de junio de 2016 (Rec. Núm. 2367/2015)
- STS Sala de lo Civil 557/2015, de 20 de octubre de 2015 (Rec. Núm. 2158/2014)
- STS Sala de lo Civil 553/2015, de 14 de octubre de 2015 (Rec. Núm. 1257/2014)
- STS Sala de lo Penal 532/2015, de 23 de septiembre de 2015 (Rec. Núm. 648/2015)
- STS Sala de lo Civil 244/2015, de 13 de mayo de 2015 (Rec. Núm. 846/2014)
- STS Sala de lo Civil 487/2014, de 30 de septiembre de 2014 (Rec. Núm. 18/2014)
- STS Sala de lo Civil 341/2014, de 1 de julio de 2014 (Rec. Núm. 1365/2012)
- STS Sala de lo Civil 421/2013, de 24 de junio de 2013 (Rec. Núm. 1220/2012)
- STS Sala de lo Civil 212/2003, de 17 de enero 2003 (Rec. Núm. 2083/1997)
- STS 282/2009, 29 de abril de 2009 (Rec. Núm. 1259/2006)
- STC 96/2012, de 7 de mayo de 2012 (BOE núm. 134 de 5 de junio de 2012)
- STC 292/2000, de 30 de noviembre de 2000 (BOE núm. 4 de 4 de enero de 2000)
- STC 290/2000, de 30 de noviembre de 2000 (BOE núm. 4 de 4 de enero de 2001)
- STC 115/2000, de 5 de mayo de 2000 (BOE núm. 136 de 7 de junio de 2000)
- STC 39/2016, de 3 de marzo de 2016 (BOE núm. 85 de 8 de abril de 2016)
- STS 948/2011, de 16 de enero de 2012 (Rec. Núm. 2243/2008)
- STS Sala de lo Civil 372/2014 de 7 de julio de 2014 (Rec. Núm. 2103/2014)
- STC 37/2011, de 28 de marzo de 2011 (BOE núm. 101 de 28 de abril de 2011)
- STSJ de Castilla y León Sala de lo contencioso 862/2018, de 28 de febrero de 2018 (Rec. núm. 210/2018)
- SPI núm. 4 de Lugo de 11 de febrero de 2021
- SPI núm. 8 de Alicante de 8 de febrero de 2021
- SPI núm. 16 de Granada de 4 de febrero de 2021

- SPI núm. 6 de Santiago de Compostela de 20 de enero de 2021

- Auto del Juzgado de Primera Instancia número 16 de Granada de 4 de febrero de 2021

- Escrito del Valedor del Pueblo "Valedor do Poblo" a la Consejeria de Sanidad "Consellería de Sanidade" de 2 de noviembre de 2020 sobre el expediente núm. I.5.Q/2902/20

- Sentencia del Tribunal Constitucional Federal alemán 1 BvR 16/13, de 6 de noviembre de 2019

- Sentencia del Tribunal Federal de Justicia alemán ZR 183/17 del 12 de julio de 2018

INFORMES JURÍDICOS Y RESOLUCIONES:

- COMISARIO PARA LOS DERECHOS HUMANOS DEL CONSEJO DE EUROPA. Informe tras su visita a España del 3 al 7 de junio de 2013

- AEPD. Informe jurídico núm. 80/2021 de 29 de marzo de 2022

  AEPD. Informe jurídicos núm. 2/2022 de 29 de marzo de 2022

- AEPD Informe jurídico núm. 2021/0038, de 17 de junio de 2020

- AEPD. Informe jurídico núm. 0036/2020 de 8 de mayo de 2020

- AEPD. Informe jurídico núm. 0017/2020 de 12 de marzo de 2020

- AEPD. Informe jurídico núm. 0017/2020 de 12 de marzo de 2020

- AEPD. Informe jurídico núm. 2020/0086 de 22 de febrero de 2020

- AEPD. Informe jurídico núm. 2018/0121 de 9 de enero de 2019

- AEPD. Informe jurídico núm. 073667/2018 de 5 de marzo de 2018

- AEPD. Informe jurídico núm. 210070/2018 de 19 de diciembre de 2018

- AEPD. Informe jurídico núm. 178/2014 de 8 de julio de 2014

- AEPD. Informe jurídico núm. 0268/2011 de 1 de septiembre de 2011

- AEPD. Informe jurídico núm. 0029/2011 de 14 de marzo de 2011
- AEPD. Informe jurídico núm. 0046/2010 de 6 de abril de 2010
- AEPD. Informe jurídico núm. 0317/2009 de 16 de febrero de 2010
- AEPD. Informe jurídico núm. 0584/2009 de 21 de enero de 2010
- AEPD. Informe jurídico núm. 0278/2009 de 3 de junio de 2009
- AEPD. Informe jurídico núm. 365/2006 de 10 de agosto de 2006
- AEPD. Informe Jurídico núm. 189/2003 de 4 de agosto de 2003
- AEPD. Resolución de procedimiento sancionador núm. PS/00070/2019 de 13 de enero de 2021
- AEPD. Resolución procedimientos sancionador núm. PS/00235/2019 de 21 de febrero de 2020
- AEPD. Resolución procedimientos sancionador núm. PS/00270/2019 de 24 de enero de 2020
- AEPD. Resolución procedimientos sancionador núm. PS/00405/2019 de 8 de enero de 2019
- AEPD. Resolución procedimientos sancionador núm. PS/00025/2019 de 23 de diciembre de 2019
- AEPD. Resolución procedimiento sancionador núm. PS/00404/2018 de 23 de diciembre de 2019
- AEPD. Resolución procedimiento sancionador núm. PS/00307/2018 de 8 de mayo de 2018
- AEPD. Resolución R/00253/2022 de 10 de junio de 2022 (expediente núm: EXP202101463)
- AEPD. Resolución R/00103/2019 de 28 de mayo de 2019 (Procedimiento núm. AP/00060/2018)
- AEPD. Resolución R/01773/2018 de 8 de enero de 2019 (Procedimiento núm. TD/01234/2018)

- AEPD. Resolución R/01422/2018 de 8 de octubre de 2018 (Procedimiento núm. TD/01051/2018)

- AEPD. Resolución R/01620/2018 de 5 de octubre de 2018 (Procedimiento núm. TD/01026/2018)

- AEPD. Resolución R/01583/2018 de 20 de septiembre de 2018 (Procedimiento núm. TD/00946/2018)

- AEPD. Resolución R/01463/2018 de 27 de agosto de 2018 (Procedimiento núm. TD/01032/2018)

- AEPD. Resolución R/01237/2018 de 5 de julio de 2018 (Procedimiento núm: TD/00685/2018)

- AEPD. Resolución R/00847/2018 de 18 de mayo de 2018 (Procedimiento núm. TD/00297/2018)

- AEPD. Resolución R/01455/2018 de 27 de agosto de 2017 (Procedimiento núm. TD/00917/2018)

- APDCAT. Dictamen CNS 8/2019 de 18 de febrero de 2019

- AVPD. Dictamen D19-008 de 30 de mayo de 2019 (Expediente CN19-003)

- AVPD. Dictamen D09-051 de 26 de octubre de 2009 (Expediente CN09-044)

- Orden judicial del Garante contra la Autoridad Sanitaria Local de Emilia-Romaña de 27 de mayo de 2021 (núm. 211)

DOCUMENTOS OFICIALES:

- AEPD. Guía de privacidad desde el diseño, 5 de octubre de 2019

- AEPD. Guía para clientes que contraten servicios de Cloud Computing, 2018

- AEPD. Guía para el cumplimiento del deber de informar, 25 de mayo de 2018

- AEPD. Memoria del año 2000

- APDCAT. Dictamen en relació amb la consulta d'un centre sanitari sobre la necessitat del consentiment en el cas de la utilització de dades de salut seudonimitzades en investigació biomédica CNS 15/2019, de 14 de mayo de 2019

- APDCAT. Guia de protecció de dades per a pacients i usuaris dels serveis de salud, junio de 2020

- APDCAT. Guía para el cumplimiento del deber de informar en el RGPD, 10 de diciembre de 2018

- ARARTEKO. Recomendación general 9/2013 de 5 de noviembre

- CBE. Informe sobre los requisitos ético-legales en la investigación con datos de salud y muestras biológicas en el marco de la pandemia de Covid-19, 28 de abril de 2020

- CdE. Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data, 23 de enero de 2017

- CEPD. Dictamen 3/2019 sobre las preguntas y respuestas acerca de la relación entre el Reglamento sobre ensayos clínicos (REC) y el Reglamento general de protección de datos (RGPD) artículo 70, apartado 1, letra b), 23 de enero de 2019

- CEPD. Directrices 03/2020 sobre el tratamiento de datos relativos a la salud con fines de investigación científica en el contexto del brote de COVID-19, 21 de abril de 2020

- CEPD. Directrices 1/2018 sobre la certificación y la determinación de los criterios de certificación de conformidad con los artículo 42 y 43 del Reglamento, 4 de junio de 2019

- CEPD. Directrices 4/2019 relativas al artículo 25 Protección de datos desde el diseño y por defecto, 20 de octubre de 2020

- CEPD. Directrices 5/2020 sobre el consentimiento en el sentido del Reglamento (UE) 2016/679, 4 de mayo de 2020

- COMISIÓN EUROPEA. Libro Blanco sobre la inteligencia artificial: un enfoque europeo orientado a la excelencia y la confianza, 19 de febrero de 2020

- COMISIÓN EUROPEA. Libro verde sobre sanidad móvil, 2 de mayo de 2014

- CRPD. Examen de los informes presentados por los Estados partes en virtud del artículo 35 de la Convención: Observaciones finales del Comité sobre los Derechos de las personas con Discapacidad, 19 de octubre de 2011

- CRPD. Observación general nº 1 (2014), de 19 de mayo de 2014

- GRUPO DI LAVORO ISS BIOETICA COVID-19. Sorveglianza territoriale e tutela della salute pubblica: alcuni aspetti ético-giuridici, (Rapporto ISS COVID-19 n.34/2020), 25 de mayo 2020

- GRUPPO DI LAVORO ISS BIOETICA COVID-19. Etica della ricerca durante la pandemia di COVID-19: studi osservazionali e in particolare epidemiologici, (Rapporto ISS COVID-19 n.42/2020), 29 de mayo 2020

- GRUPPO DI LAVORO ISS BIOETICA COVID-19. Protezione dei dati personali nell´emergenza COVID-19, (Rapporto ISS COVID-19 n.42/2020), 28 de mayo 2020

- GRUPPO DI LAVORO ISS BIOETICA COVID-19. Supporto digitale al tracciamento dei contatti (contact traicing) in pandemia: considerazioni di ética e di governance, (Rapporto ISS COVID-19 n.59/2020), 17 de septiembre de 2020

- GT29, Opinión 3/2010 sobre el principio de responsabilidad (WP 173), 13 de julio de 2010

- GT29. Dictamen 02/2013 sobre las aplicaciones de los dispositivos inteligentes, 00461/13/ES (WP 202), 27 de febrero de 2013

- GT29. Dictamen 05/2014 sobre técnicas de anonimización, 0829/14/ES (WP216), 10 de abril de 2014

- GT29. Dictamen 15/2011 sobre la definición del consentimiento, 01197/11/ES (WP 187), 13 de julio de 2011

- GT29. Dictamen 4/2007 sobre el concepto de datos personales, 01248/07/ES (WP 136), 20 de junio de 2007

- GT29. Dictamen 8/2014 sobre la evolución reciente de la Internet de los objetos, 1471/14/ES (WP 223), 16 de septiembre de 2014

- GT29. Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679, 17/ES (WP251), 6 de febrero de 2018

- GT29. Directrices sobre el derecho a la portabilidad de los datos, 16/ES (WP 242 rev.01), 13 de diciembre de 2016

- GT29. Directrices sobre la transparencia en virtud del Reglamento (UE) 2016/679, 17/ES (WP260), de 11 de abril de 2018

- GT29. Documento de Trabajo sobre Datos Genéticos, 12178/03/ES (WP 91), 17 de marzo de 2004

- GT29. Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), 15 de febrero de 2007

- GT29. Opinión 3/2013 sobre la limitación de la finalidad (WP 203), de 2 de abril de 2013

- GT29., Dictamen 1/2010 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento», 00264/10/ES (WP 169), de 16 de febrero de 2010

- ICO. Guide to the General Data Protection Regulation (GDPR), 2 de agosto de 2018

- INCIBE. Tecnología biométricas aplicadas a la ciberseguridad: una guía de aproximación para el empresario, 2016

- OMS. Ciudades globales amigables con los mayores: una guía, 2007

- OMS. Informe mundial sobre el envejecimiento y la salud, 2015

- PARLAMENTO EUROPEO. Resolución de 14 de marzo de 2017 sobre las implicaciones de los macrodatos en los derechos fundamentales: privacidad, protección de datos, no discriminación, seguridad y aplicación de la ley (2016/2225(INI))

- UIT. Recomendación Y.4000/Y.2060**,** 15 de junio de 2012

- UNIÓN INTERNACIONAL DEL NOTARIADO. Guía notarial de buenas prácticas para personas con discapacidad: El notario como apoyo institucional y autoridad pública, 2019